HANDBOOK

DIGITAL FINANCIAL SERVICES AND RISK MANAGEMENT

The MasterCard Foundation

IFC International Finance Corporation
WORLD BANK GROUP

ACKNOWLEDGEMENTS

The MasterCard Foundation and IFC's Partnership for Financial Inclusion Program would like to acknowledge the generous support of the participating institutions in our study; Tigo Tanzania, Kopo Kopo Kenya, FINCA DRC, Fidelity Bank Ghana, and Zoona, as well as Genesis Analytics for their work in supporting the risk assessments and contributions to the handbook. The authors would also like to thank Anna Koblanck for her extensive editing, and the IFC clients, DFS providers, and industry stakeholders who participated in interviews, including Software Group, GSMA, and CGAP. Finally, The MasterCard Foundation and IFC would like to extend special thanks to the authors, Lesley Denyes and Susie Lonie, and to the reviewers for their contributions; David Crush, Ruth Dueck-Mbeba, Justice Durland, Cameron Evans, John Gutin, Richard Ketley, Andrew Lake, Joseck Mudiri and Patricia Mwangi.

ISBN Number: 978-0-620-71506-5

HANDBOOK

DIGITAL FINANCIAL SERVICES AND RISK MANAGEMENT

The MasterCard Foundation

IFC
International Finance Corporation
WORLD BANK GROUP

01_
OVERVIEW
of risk management techniques

02_
Risk
DEFINITIONS

03_
Risk management
FRAMEWORK
applied

04_
INSIGHTS AND TOOLS

Foreword

This handbook is designed for any type of financial institution offering or planning to offer digital financial services, such as mobile money and agent banking. It could be microfinance institutions, banks, mobile network operators, or third party payment service providers. The conceptual framework for risk and risk management is based on global standards enterprise risk management and best practices (ISO 31000), but the application of principles, illustrations, and descriptions address risks from all perspectives and all types of providers. Examples and case studies are illustrative only and sometimes anonymized to mask the identity of the institution to allow a fuller description of the circumstances surrounding the events that occurred. Examples are highly characteristic of the type of institution and the specific market environment, and must be contextualized before applied in different contexts.

The handbook does not assume any prior knowledge of risk management; however it does assume a moderate understanding of Digital Financial Services and Alternative Delivery Channels, including products, the function of agents, the role of technology and regulators. For the sake of consistency, the handbook will refer to digital financial services, a broader definition that applies to many channels as well as products. A glossary can be found on page 109 for further descriptions of terms used in the handbook.

The handbook is organized in four parts:

- Part one provides the conceptual framework for risk management and key elements of the process. It also gives an overall context for DFS risk management.
- Part two describes the main types of risks faced by DFS providers, including real examples from various markets.
- Part three introduces the step-by-step process of implementing a risk management framework. It can be used to guide the initial design and deployment of a DFS strategy, as well as how to monitor and manage risks during the ongoing implementation of the strategy.
- Part four highlights lessons learned by IFC clients across Africa, and considers how digital financial services may change in the coming years and the risks and opportunities DFS present to financial service providers.

In addition, the tools chapter provides a full risk database and there is a glossary that can be used as a reference guide when developing a risk management strategy for your institution.

CONTENTS

PART IV: INSIGHTS AND TOOLS 88

ACRONYMS

ADC	Alternative Delivery Channel
AfDB	African Development Bank
AML/CFT	Anti-Money Laundering and Combating the Financing of Terrorism
API	Application Program Interface
ATM	Automated Teller Machine
DFS	Digital Financial Services
ERM	Enterprise Risk Management
GDP	Gross Domestic Product
GSMA	Groupe Speciale Mobile Association
IFC	International Finance Corporation
ISO	International Organization for Standardization
IT	Information Technology
KPI	Key Performance Indicator
KRI	Key Risk Indicator
KYC	Know Your Customer

MFI	Microfinance Institution
MNO	Mobile Network Operator
MOU	Memorandum of Understanding
NGO	Non-Governmental Organisation
OTC	Over The Counter
P2P	Person to Person
PAR	Portfolio at Risk
PIN	Personal Identification Number
POS	Point of Sale
PSP	Payment Service Provider
SIM	Subscriber Identification Module
SLA	Service Level Agreement
SMS	Short Message Service
TPS	Transactions Per Second
USD	United States Dollars
USSD	Unstructured Supplementary Service Data

Executive Summary

The last decade has seen a wave of innovative financial services aimed at serving the unbanked populations in emerging markets. Low-income individuals, micro-entrepreneurs and rural populations that were previously left out of the market due to the high costs of physical expansion are now accessing financial services through mobile phones and networks of agents acting as representatives of financial service providers. This has resulted in a remarkably rapid increase in financial inclusion in some countries. In other markets adoption has been slower and the results are less catalytic, but all markets are growing and are expected to continue to do so as services and products develop. It is expected that the expansion of digital financial services will make an important contribution towards the goal of reaching universal financial access by 2020.

However, with the many opportunities provided by ground-breaking technology and innovative business operations also come new risks. The risks related to implementing digital financial services extend far beyond operational and technical risks. In order for the financial inclusion industry to be able to capitalize fully on the benefits of digital financial services, it is important that the accompanying risks are understood and adequately addressed. In this fast evolving field, it has become apparent that what matters to one provider matters to all as large cases of fraud, for example, affect not just consumer trust in one provider but in the market and promise of digital financial inclusion as a whole.

The Partnership for Financial Inclusion is a joint initiative of IFC and the MasterCard Foundation to expand microfinance and advance digital financial services in Sub-Saharan Africa. Through the interactions with clients of the program as well as the broader industry in the region and beyond, we identified a need for a handbook on how best to handle risk management for digital financial services. There are a number of good industry publications that focus on specific risks such as fraud or regulatory risk, and some documents focused on challenges specific to certain institutions such as GSMA's Risk

Management Toolkit for Mobile Network Operators for example. There is, however, no comprehensive guide to risks associated with DFS implementations in general that in layman's terms can assist an institution in learning from the beginning what risk is, how risk affects a DFS deployment, and how to manage it. In 2015, we embarked on a series of research projects to answer these questions and to develop this handbook.

In developing this handbook, we interviewed more than thirty practitioners, software vendors and industry stakeholders, and conducted four in-depth organizational risk assessments. Most of these practitioners are based in Sub-Saharan Africa, but their experiences can also be helpful for other regions. During the research, we learned that there are very few institutions, including banks, MFIs and MNOs, with any kind of risk framework for DFS. Only one institution had developed a comprehensive risk management framework that was regularly used and reported to group level on a monthly basis. It is probably not a coincidence that it was also one of the few institutions that had not had any publicly reported fraud, small or large. We found it surprising that the banks in our sample had the lowest levels of developed frameworks, given that banks are traditionally known as risk-adverse institutions with strong risk and compliance departments. Our conclusion is that there is a strong need for financial service providers across the industry to strengthen DFS risk management practices if they are to achieve their business objectives.

Through this research initiative, it also became apparent that while risks can be described in various different categories, they are in often strongly related. Technology, strategic, and agent management risks can all lead to reputational risk, and fraud can incur even bigger financial losses from reputational damage than from the fraud itself. There were also key strategies that were identified as being the most effective in managing risk, for example the use of call centers to track, monitor, and predict eventualities; using strong reconciliation and settlement processes to reduce potential losses; and to take partnerships seriously and ensure that partners are held accountable.

This handbook uses the ISO 31000 standards for Enterprise Risk Management to establish principles for risk management of DFS. The ISO standards use a framework of 7Rs and 4Ts to develop risk frameworks, which are:

- Recognition or identification of risks
- Ranking or evaluation of risks
- Responding to significant risks
  - » Tolerate
  - » Treat
  - » Transfer
  - » Terminate
- Resourcing controls
- Reaction planning
- Reporting and monitoring risk performance
- Reviewing the risk management framework

When doing a risk assessment, it is important to look at causes of the risks and to identify trends. Prevention is much more effective than damage control after the fact. One example that came up repeatedly in our research was that a lack of business process or the lack of enforcement leads to most large-scale internal fraud. Large scale internal fraud has the power to shut down a service, as well as cause such reputational damage as to shrink the whole market. Technology is often blamed for fraud, but in many cases the opportunity for fraud is opened up by a lack of good operational practices.

Going forward, there are key trends that will dictate how we look at risk and DFS. The pace of technology enhancement and smartphone penetration will shape how services are developed and offered to the market, and regulations will continue to change with the dynamics of the market. In an increasing number of jurisdictions regulators are starting to mandate interoperability between payment services including mobile money, as well as preventing providers from signing exclusive arrangements with agents. Whilst the longer term vision is to see a reduction in the use of cash as people adopt DFS for more transactions, at present, cash remains dominant. It is therefore essential that providers continue to focus on liquidity management and allow customers to cash-out regularly, and manage the associated risks.

It is our hope that this handbook will provide useful guidance and support to organizations employing digital financial services to expand financial inclusion. Good management of the risks involved is necessary for the opportunities of new technology and business models to be fully realized for the benefit of providers, partners, customers and emerging economies alike.

Introduction

IFC supports institutions seeking to develop digital financial services for the expansion of financial inclusion, and is engaged in a multitude of initiatives across a range of markets through its portfolio of investments and advisory projects. In Sub-Saharan Africa, many advisory projects are implemented in partnership with The MasterCard Foundation in a joint initiative that also includes a comprehensive research agenda. Much of the early learning from these projects was captured in the Alternative Delivery Channels and Technology Handbook[1] which provides a comprehensive guide to the components of a DFS strategy and, in particular, how to understand the technological building blocks for a successful deployment. In conjunction with supporting the expansion of financial inclusion through DFS, it is important to ensure their sustainability and reliability via the implementation of effective and responsible risk management practices.

The research for this handbook included three components; interviews with approximately 30 practitioners; four in-depth case studies with Tigo Tanzania (MNO), FINCA DRC (MFI), Kopo Kopo Kenya (PSP) and Fidelity Bank in Ghana; and a two-day client workshop held in Cape Town in November 2015. The research objectives were to:

- Clearly define and describe all types of risk that may be faced by financial service providers using DFS.
- Provide easy-to-use guidelines for conducting risk diagnostics, assessments, developing risk frameworks, and implementing risk management tools.
- Analyze how different types of financial institutions currently assess risk and implement risk management tools.
- Identify general lessons learned by financial service providers about DFS risk management that are relevant to other markets and organizations on such issues as integration with exiting institution-wide risk frameworks; key risk indicators; most common types of risks faced; how best to mitigate risk; and best practices for DFS risk management.

We found that although most providers have extended their existing risk frameworks to include alternative channels, there is only a nascent understanding of the additional risk that DFS bring. This is particularly pertinent as DFS deployments often mean that organizations engage in business activities outside of their core business, such as mobile network operators offering financial services through mobile wallets, or banks and MFIs partnering with MNOs to offer traditional banking products through new channels. There is a growing need for guidance about DFS risk management that is relevant and accessible to all types of providers.

There are several excellent reference documents that give technical detail about the creation of a risk management framework (see page 111) and this publication does not seek to replicate these. Our focus is to describe the basic underlying principles of risk management for practitioners who are not risk specialists but are involved in the establishment and protection of a DFS business. As with any new service, there is much to be learned and many challenges and unanticipated risks to be addressed. This handbook serves as a practitioners guide to identifying, assessing, and mitigating risks specific to DFS.

[1] Alternative Delivery Channels and Technology Handbook, IFC, 2015

01_

PART 1

Overview of Risk Management Techniques

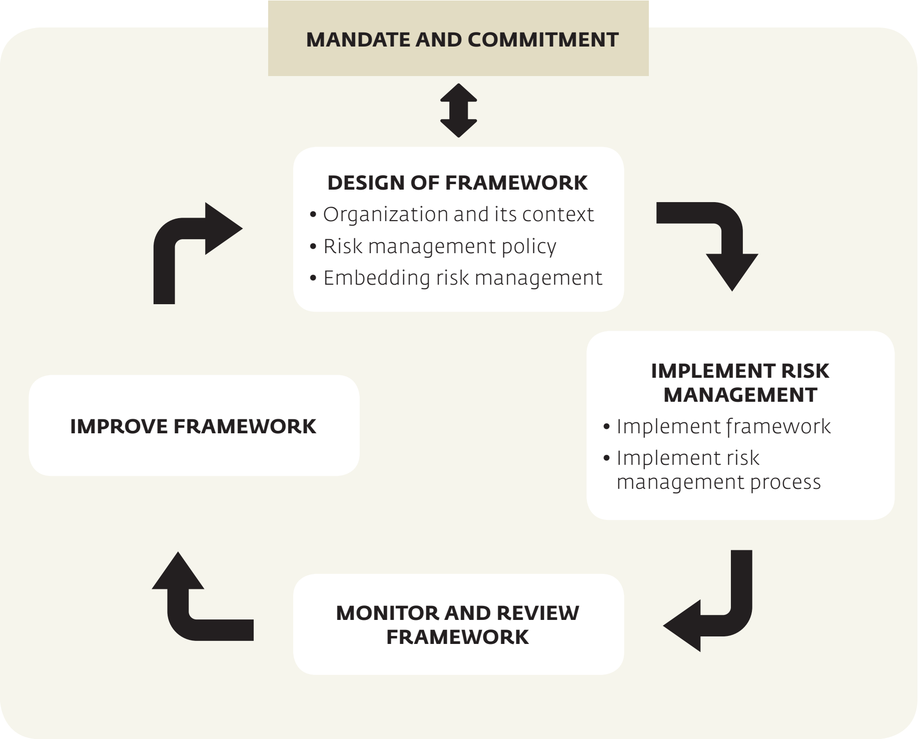
Risk can be described[2] as the "effect of uncertainty on objectives". There are many definitions, approaches, and frameworks used across various businesses and industries, with one of the key global standards being ISO 31000. The consequences of a change in circumstances or events may be positive or negative. This section of the handbook lays out the conceptual principles of a risk management framework, the risk assessment process, and the key components of developing a risk management framework for DFS.

Risk management begins with the mandate and commitment of the management and governance bodies of the institution, and is followed by design of a framework, implementing risk management, monitoring and review of framework, and lastly, continuously improving the framework. Establishing an effective risk framework is an essential aspect of good corporate governance for all companies and should be a key priority for boards of directors and senior management. The implementation of a risk management framework requires the appropriate risk department for the size of and complexity of the organization. Almost all financial institutions are required to have a head of risk management, with officers or departments responsible for different areas of risk. For DFS, the area that is generally least developed is operational risk, and this requires the greatest attention. The teams involved in managing the DFS operations have the greatest awareness of what is required and what can go wrong and should be included as early as possible in the planning process of a DFS risk strategy. This provides a very useful counterbalance to the business development teams who often fail to anticipate the risks in the strategies that they are promoting or see risk assessment as an impediment to progress.

[2] ISO Guide 73 from ISO 31000

> *"Risk management begins with the mandate and commitment of the management."*

Figure 1: *Framework for managing risk (based on ISO 31000)*



MANDATE AND COMMITMENT

DESIGN OF FRAMEWORK
- Organization and its context
- Risk management policy
- Embedding risk management

IMPLEMENT RISK MANAGEMENT
- Implement framework
- Implement risk management process

MONITOR AND REVIEW FRAMEWORK

IMPROVE FRAMEWORK

Source: AIRMIC, Alarm, IRM: 2010

Risk Management Frameworks

All businesses are subject to a range of risks, some of which are anticipated but many of which are either unexpected or not effectively managed. Adopting a formal risk management framework can assist businesses in planning more effectively, understanding why things have not gone according to plan and, ideally, in taking action before losses are incurred. The goal in having an effective risk management framework is to be pro-active rather than reactive in managing the risks inherent in a business model.

As per ISO 31000, there are seven Rs and four Ts of risk management frameworks:

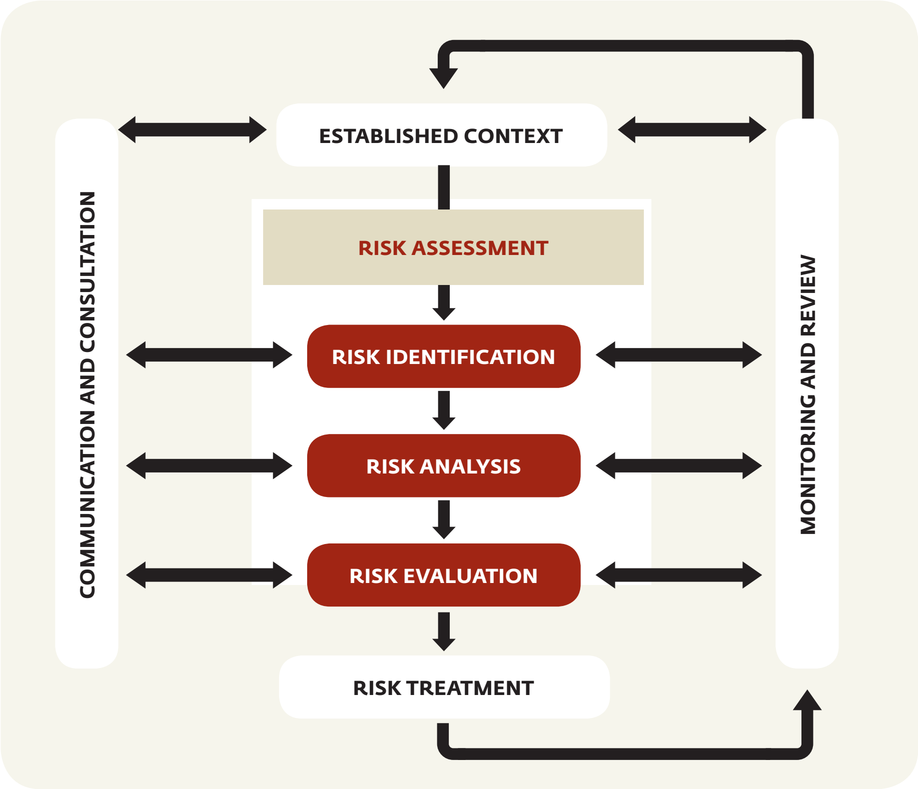
- Recognition of risks: The brainstorming and identification of all types and subtypes of risk events that may occur and impact the DFS implementation;
- Ranking or evaluation of risks: The use of qualitative criteria based on probability and potential impact to rank risks based on highest to lowest importance;
- Responding to significant risks: the development of risk strategies based on probability and potential impact:
  - » Tolerate: For risks with low probability and low potential impact, risks can be accepted or tolerated as the cost of mitigating or eliminating the risk may be higher than its potential impact.
  - » Treat: For risks with moderate probability and potential impact, treatment can be applied to mitigate the potential loss from events occurring.
  - » Transfer: For risks with high probability and high potential impact, the risk can be transferred to a third party by outsourcing or purchasing of insurance.
  - » Terminate: For risks with very high probability and potential impact, the risk can be terminated by discontinuing the DFS offering or by taking recourse such as sourcing new partners or vendors.
- Resourcing controls: The development of budgets to apply to risk responses.
- Reaction planning: The development of tactical risk responses.
- Reporting and monitoring risk performance: Period reporting on risk performance to state whether the risk has occurred and losses have happened, it has occurred and been mitigated; or it has not yet occurred.
- Reviewing the risk management framework: The process of reviewing and re-iterating the risk management periodically or when significant events occur.

Risk management frameworks are a comprehensive set of policies aimed at reducing the impact of risks associated with DFS. The framework is a culmination of all planning and assessment processes, and the risk register is the main body and working document. The methodology for development of a risk management framework can be found in Part III of this handbook.

Risk Assessment Process

The development of a Risk Management Framework involves conducting a risk assessment process of identification, evaluation, and development of risk treatment strategies for risks associated with DFS.

Figure 2: Risk Assessment Process



Source: AIRMIC, Alarm, IRM: 2010

A risk management framework begins with establishing a *context* of risks; it should seek to *identify* and classify the risks involved (and ideally measure risks); evaluate, assess, and *analyze* the risks; *evaluate* and plan to minimize these risks; develop risk *treatments*; and *monitor* and review the results of risk treatment.

The final output of a risk assessment is a risk management framework including a risk register. Also known as a risk matrix, the term risk register is used interchangeably to describe the central database of identified risks, along with their descriptions, causes, effects, and policies - whether it be to tolerate, treat, transfer or to terminate. Risk registers are central to a risk management framework as they capture all possible events and allow users to monitor, report, and reassess risks on an on-going basis. Risk registers also allow providers to lay out all sub-levels of risk and to create risk strategies so that if one level of an event occurs, there is a strategy to prevent it from entering to the next level, such as malware that infiltrates a system but is stopped from gaining access to sensitive data.

Risk registers include:

RISK CATEGORY
Strategic, Regulatory, Operational, Technology, Financial, Political, Fraud, Agent Management, Reputational or Partnership Risk

RISK NAME
Clearly defined name of the risk identified

DESCRIPTION
Elaborated description of the risk

OWNER
Person responsible for monitoring the risk and implementing risk treatment strategy

CAUSE
The event, if it occurred, that would result in the risk being actualized

EFFECT
The impact that the event would lead to if it occurred

RISK STRATEGY
Tolerate, Treat, Transfer or Terminate

RISK TREATMENT STRATEGY
The strategy on how to mitigate or control the risk

TREATMENT TACTICAL RESPONSE
The policy or procedure implications of the risk treatment strategy

KEY RISK INDICATOR
An indicator used for the early warning that the adverse effects of the particular risk may occur

CURRENT STATUS
Whether the risk event has not yet occurred; has occurred and been successfully treated; or has occurred and caused losses.

Examples have been given in the next section to illustrate this process. The risk register is a living document that is re-assessed and updated on a pre-defined period basis or on occurrence of a major or unexpected event. It is used as the knowledge body of risks for the institution and its DFS implementation. A template for a risk register can be found in the Tools section of this document.

02_

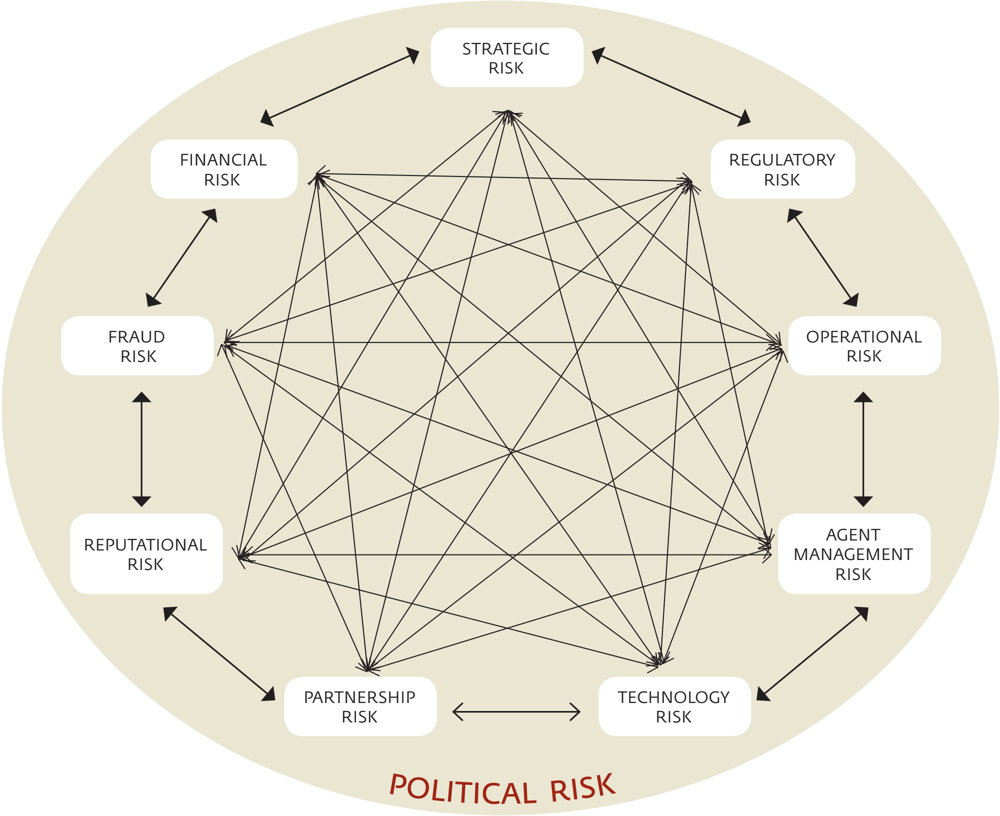
Part II

Risk Definitions

The potential for DFS comes with inherent risks as operations and client interactions are outsourced to agents who open accounts and conduct transactions on behalf of the provider. In recent history, a few notable fraud cases have affected the reputation and financial viability of some operations. While fraud risk is the most notorious and best understood risk associated with DFS, there are many others that are not always incorporated in a provider's risk management framework although they can be as damaging. These include: strategic, regulatory, operational, technology, financial, political, agent management, reputational, and partnership risks.

Each of these risk categories are described and explained in this section, including a substantial number of sub-categories. With each risk, appropriate risk mitigation strategies are also identified and explored. Case studies and practical examples provide a deeper understanding of the concepts. Each risk category also illustrates how a risk register could be used to document key elements such as risk identification, risk ownership, risk assessment, risk treatment, and risk indicators, as part of an organization's risk management strategy. A helpful checklist asks the reader critical questions and challenges them to reflect on their own organizational risks.

Figure 3: Risk Categories and Interactions



Risks do not fall strictly in one category. If a risk situation arises in one area it can often create a risk situation in another area, and all risks must be considered together. For example, poor strategic decisions regarding the service and the technology selection can lead to technology risk which in turn leads to many other kinds of risk, such as operational and agent management risk if there are not appropriate back office systems, or fraud risk if the expected fraud prevention features are not delivered, or reputational risk if the customer experience is poor. Therefore, a strategic need to reduce fraud risk may also lead to a need for risk prevention measures in operations, technology, agent management and so forth.

What is your risk appetite and tolerance?

1. Strategic Risk

Strategic risk is broadly defined as the actual losses that result from the pursuit of an unsuccessful business plan or the potential losses resulting from missed opportunities. Some examples of this may be ineffective products, failure to respond to change in the business environment, or inadequate resource allocation.

As dependence on technology grows, providers become increasingly exposed to risk resulting from innovation and disruptive technologies in the market. Setting company strategy is generally the responsibility of the board, which should bring its experience of other companies and industries to bear in identifying the risks to the company's DFS strategy. Strategic risks include those related to branding, economic trends, reputation, business models, and competitive positions. It is also related to technology, which requires a reputable, usable, scalable, and secure system to minimize strategic risk.

Providers need to have a deep understanding of the nature and breadth of risks related to their business strategy and the tolerance for their potential impact. To address strategic risk, providers must focus on gathering data and appreciating external perspectives from outside sources including customers, bloggers, information trendsetters, competitors, and marketplace analysts. For many DFS offerings, the competition may be quite different from that of the core organization, and these new competitors must be identified and understood. Financial models can be used to build scenario analysis and stress testing to further understand the key drivers of the profitability such as volume, value, revenue, and costs.

How to develop a risk register is outlined in Part III. Below is an example of a strategic risk in a risk register and includes the category, description, owner, cause, effect, probability, impact, strategy, and Key Risk Indicator.

EXAMPLE 1

Risk Register

Strategic Risk – unrealistic business case

DFS Provider example:	MNO that offers a mobile money wallet
Risk Category:	Strategic Risk
Secondary Category:	Reputational
Name:	MNO mobile wallet fails to reach sustainability in the timeframe designated
Description:	The DFS does not meet revenue and expense targets and results in negative net revenue and return on investment.
Owner:	Head of Mobile Money
Cause:	Poor product or channel design, misunderstanding of market demand and/or competition
Effect:	Loss of investment
Probability:	2 out of 5 *Fairly low probability based on market research and financial modeling*
Impact:	3 out of 5 *Medium impact based on that operations will likely be given opportunities to address the problems to fix before operations are ceased*
Risk Strategy:	Treat
Treatment Strategy:	• Use market research and industry benchmarks to base assumptions • Iterate financial model as implementation progresses • Ensure targets are disseminated and aligned with KPIs • Monitor performance and update strategy as needed
Treatment Tactical Response:	• Determine the causes of under-performance (product design, market response) and create resolution plans • Adjust business case and targets to reflect the new phase of the product life cycle
Key Risk Indicator:	• Net revenue • Active customers • Transactions per customer • Active agents • Customers per agent • Float interest rate
Current status:	Has not occurred

Box 1

Strategic Risk Case Studies

A) Launching a poorly defined service: When the first mobile money service in Sub-Saharan Africa was launched it quickly gained enormous popularity, and was seen by the MNO service provider as a significant "churn-buster" that would protect its core telecoms business via increased customer acquisition and retention. As a result, many African MNOs were concerned about the strategic risk to their core business if they did not offer a similar service. This caused many MNOs to launch mobile money services without properly understanding the market, the customer proposition, the technical functionality needed, or the resources required to provide a successful service. The ironic result of this was that they were subjected to the consequences of a different strategic risk by entering a new market for which they were ill prepared and were providing poor quality services.

Symptoms of hurried implementation and poor execution of strategic decisions can be seen in the many unsuccessful services launched in the early days. The market exploded with over 200 services launched or in development in the first five years with perhaps five percent achieving something close to resembling success. The situation is improving, but there are still many services that suffer as a direct result of these poor decisions in the form of understaffing and insufficient budget to develop the business and struggling with inappropriate technology.

B) Loss of core telecoms business: It is generally the case that in order to register for an MNO mobile money service, the customer has to subscribe to that MNO telecoms business and use its SIM card. This provides obvious commercial benefits to the MNO in customer acquisition and retention, but also restricts the potential maximum size of the DFS to the size of the MNO client base, and if the core telecoms business declines, so too does the mobile money business. In the early days of mobile money, many MNOs considered the key benefit of DFS to be its potential to provide a point of difference that enhanced the attractiveness of their core telecoms business. Nowadays, most MNOs in Sub-Saharan Africa offer mobile money as part of their portfolio, so it no longer provides that differentiation unless it has some compelling benefit not offered by the competition.

Tanzania has several successful MNOs, and competition in the telecoms space is fierce. Many customers have multiple SIM cards and use the one that offers the best deal at the time. All offer similar mobile money services and it is common for customers to register for multiple mobile money accounts[3]. There is therefore a real issue that when an MNO offers a sustained attractive telecoms deal to customers, the DFS business also grows, whilst the competition's DFS suffers by default. In order to mitigate this risk, added value DFS are being introduced in many markets including savings accounts, access to loans, and profit sharing on the funds held in accounts.

C) Growing "Direct Deposit" transactions: The standard process for remitting funds via a wallet is that the customer deposits cash at an agent, and then remits the funds by performing a Person-to-Person transaction. Whilst the deposit is usually free, nearly all services exact a charge for each P2P transfer. It is possible for customers to bypass the P2P transaction and avoid this charge at the point when they cash in by giving the agent the phone number of the recipient wallet instead of their own. Funds are deposited directly into the recipient account without ever touching that of the person making the deposit. This is against the terms of operation because there is no record of the sender's identity, which can infringe KYC regulations. Bypassing the P2P transaction can also have a serious negative impact on the business revenue model. The agent needs to be paid commission for providing the cash in service, and this is typically financed, at least in part, by the P2P revenue. Further, the sender need not even be a mobile subscriber.

Direct deposits are therefore the source of potential regulatory and financial risk, but arguably the biggest impact is that they undermine the DFS strategic role of supporting and protecting the core telecoms business. Most MNOs are suffering from increasing levels of direct deposits. Some agents are actively complicit in providing direct deposits, while others are unaware that it is happening. Efforts are being made to identify the offending agents by tracking whether a withdrawal happens soon after the deposit and in another location. There seems little rationale for cashing in and out in quick succession, and if the cash out took place far from the cash in, the transaction was probably a direct deposit. Another approach is to track the location of the agent and the recipient of the deposit using cell ID; different locations again suggest a direct deposit. Agents prone to high levels of direct deposits are cautioned, and withdrawn from service if necessary. This detection process is time consuming and labor intensive, but currently the best means available to protect the business from the risk from direct deposits.

STRATEGIC RISK – KEY QUESTIONS

- How well is my strategy actually defined?
- How broad are the risks that we are considering? Have we considered all internal and external factors?
- What risk scenarios have we considered to test our plans?
- What is our risk appetite and tolerance?
- Have we mapped our risks to key performance indicators and value measures?

[3] In 2014, Tanzanian DFS users had on average 2 mobile money accounts http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2014/03/Tanzania-Enabling-Mobile-Money-Policies.pdf

Have I identified potential areas for risk of non-compliance?

2. Regulatory Risk

Regulatory risk refers to the risks associated with complying (or not complying) with regulatory guidelines and rules, such as anti-money laundering/combating financing of terrorism, Know Your Customer, data privacy, account and transaction limits, trust accounts, and regulations regarding the use of agents. Regulatory risk also includes broader rules relating to the operation of a particular institution such as, for example, licensing, capital and liquidity. Non-compliance may be in areas that are not directly related to DFS but can have significant impact on business operations including fines, penalties, and even loss of license. Each country's central bank sets the requirements for mobile banking, mobile money, and agent banking within their jurisdiction[4] . These generally include policies that govern DFS, often a national payments act, financial inclusion act, or customer protection act. Central banks in each country decide if they will allow banks, MNOs, payment service providers, or a combination of these, to provide services through DFS. In addition to the types of institutions that will be allowed to offer services, central banks also dictate requirements on the following topics:

Customer Due Diligence: One of the key areas covered by DFS regulations is customer due diligence, including KYC, anti-money laundering, and combating the financing of terrorism. These regulations can also be major obstacles to developing and scaling digital financial services in emerging markets, for example hindering the customers' ability to register for a service because of poor quality personal identification documents, insufficient proof of residence, or lack of biometric verification tools.

Several central banks around the world have allowed for tiered KYC as a means of introducing proportionality into the risk management of mobile services. The risk of large amounts of money being funneled through mobile accounts for money laundering or financing of terrorism is likely to be limited as most accounts are capped as low-value accounts, can be traced to mobile phone numbers with amounts and date, require security PINs, and are continuously monitored. Tiered KYC takes a risk-based approach and extends proportional access to the account based on the level of KYC requirements. Proportional limits are placed on the amount per transaction, account turnover per day, month or year, and on the maximum balance that can be held at any one time.

Agent Management: The use of agents to act on behalf of financial institutions is strictly governed by regulators in most markets. There may be business requirements for signing up agents, including whether they are registered or licensed, minimum capital requirements, or even restrictions on the type of business. Regulators also dictate the

[4] In a few markets these regulations are still in development and not yet implemented.

functions that can be performed at agents, for example whether they can open accounts or not, collect KYC data, conduct cash in and cash out transactions, or perform over-the-counter transactions. The regulator may include stipulations regarding the exclusivity of agents, for example mandating that agents cannot be exclusive to a single financial institution.

Agent management regulations vary from country to country. In some countries, agent banking and e-money regulations are clearly established and include full requirements for the recruitment, approval, training, and on-going management of agents. In countries such as Tanzania, the regulator has to individually approve each agent that a bank or MFI recruits. In other markets, such as Madagascar, there are currently no regulations and the Central Bank has not given any formal indication of what is allowed or prohibited regarding the types of agents to be recruited, their business requirements, or what functions they are allowed to perform. In markets like these, regulatory risk becomes one of the primary risks to a DFS implementation, as institutions operate under completely unknown circumstances.

In addition to the regulatory risks associated with agents, there are several other types of risk that are detailed in the Agent Management Risk section of this document.

Deposit Insurance: Deposit insurance is insurance provided to depositors to protect their deposits in cases of financial institution insolvency. It is usually a mandatory part of the laws governing financial institutions, as the protection of customer deposits is key to deterring bank runs and maintaining a stable financial sector. Deposit insurance is not typically required by central banks for MNOs or payment providers as they are not allowed to intermediate the funds and the wallet balances are 100 percent backed in trust accounts, usually held in third party financial institutions.

Privacy: As with all financial services, protection of customer data is paramount and can be mitigated through IT system access control and encryption to protect data abuse by the provider's staff. Privacy regulations may be addressed through national privacy laws, telecommunication regulations, and/or financial services regulations. Data privacy is an increasing concern for institutions as large, public data hacks have been well documented in the media, causing both financial and reputational losses. Lack of integrity around customer data can lead to lawsuits, as well as providing opportunities for identify theft and fraud.

Interoperability: Interoperability is defined as the ability for a user of one account or wallet from a provider to receive or send transfers to a user's account or wallet of another provider. Interoperability may also be described at the agent level, when a customer from one provider can transact at the agent of another provider. Most regulators have not mandated interoperability amongst domestic providers, but some have instead left the market to self-regulate interoperability. As markets mature, we may see more mandated interoperability as regulators aim to intensify competition in an attempt to increase customer options and reduce prices. In Sub-Saharan Africa, interoperable "account to account" domestic transfers are currently available[5] in Tanzania, Rwanda, and Madagascar.

Trust Accounts: All non-bank DFS providers, including MNOs and payment service providers, are approved by the regulators, either through licensing or 'no-objection letters', by a central bank, securities and exchange commission, or a communications regulator with provisions for holding funds in one or many trust accounts. Funds are matched one-to-one between the e-money and the funds held in the bank and the providers are not permitted to intermediate the funds the way a regulated financial institution would. The purpose is to ensure that customer funds are protected and readily available upon request. These funds are ring-fenced and providers are unable to use them to pay for operational expenses or to pay creditors. Depending on the regulation, interest earned on the trust account may have to be paid to the customer or may be used as revenue for the provider.

Minimum Capital Requirements: For banks, minimum capital requirements are a normal part of regulatory requirements for licensing. In some markets, regulators also require them for MNOs and PSPs. In addition to requirements for MNOs and PSPs to hold funds in trust accounts, regulators may also impose minimum capital requirements in order to insure creditors against insolvency risk and to ensure that the institution has enough capital to see through operational costs of start-up.

[5] GSMA report: State of the Industry 2015

EXAMPLE 2

Risk Register

Regulatory Risk – inadequate customer registration

DFS Provider example:	MNO that offers a mobile money wallet
Risk Category:	Regulatory Risk
Secondary Category:	Agent Management Risk
Name:	Agent does not adequately register customer with full KYC procedure
Description:	Agents may not fully comply with KYC requirements as commissions are designed to incentivize account opening and performing transactions, not regulatory diligence.
Owner:	Head of Compliance
Cause:	Poor product or channel design, poor agent training
Effect:	Increased expenses to follow up and collect KYC data or account closure if these cannot be adequately registered
Probability:	3 out of 5 *Medium probability based on good training, but common issue*
Impact:	1 out of 5 *Very low impact based on regulators likely response to give warnings before violations are punished*
Risk Strategy:	Treat
Treatment Strategy:	• Agent education • Align agent incentives to fully registered accounts only • Redesign business processes to be more efficient in managing any documentation • Where regulations allow, open accounts at lower KYC levels until full information can be collected • Mystery shopping • Penalties for non-compliance
Treatment Tactical Response:	• Additional agent training • Invoke penalties to agents and/or agent management officers
Key Risk Indicator:	• Percentage of customers with incomplete registrations • Percentage of customers with rejected registrations
Current status:	Occurred and mitigated

Box 2
Regulatory Risk Case Studies

The most common regulatory risks are caused by the two extremes of "no regulation" and "over-regulation", both of which can lead to wasted investment and lost revenue.

In markets where there is little or no clear oversight of DFS, there is uncertainty about what the regulator requires or what regulations may be imposed at a later date. For example, a major MNO decided to launch its successful African mobile money service in a large South Asian market targeting a 2008 launch. Legal opinion was that in the absence of specific regulation, a suitable framework could be constructed to adhere to more general payments regulation. A substantial amount of money was invested in tailoring the existing technology to the specific needs of the market and a large team was recruited and trained to manage local operations. Just two months before the planned launch in the first state, the regulator issued some new guidelines to existing regulation that effectively prohibited the launch. Despite intense negotiations, the launch was delayed and eventually cancelled, and the team disbanded. Three years later the regulation had again been modified and the service was eventually launched. The cost to the MNO of the delay, both direct and as lost revenue, has not been disclosed.

In one African market, the central bank decided that it would impose certain regulatory constraints on any mobile money deployment with the intention of ensuring that there would be full interoperability between services from the start, and that the potential risks and rewards associated with each service would be shared between several local banks. Unfortunately, the regulator was unfamiliar with the state of the technology in this nascent market and had assumed that it had a range of functionality and capabilities that was not going to be commonly available for several years. In addition, the business case for these services relied upon a "closed-loop" environment with just one revenue earner. As a result, what was expected to be one of the leading DFS markets has struggled to gain traction and had poor uptake for several years until the regulation was modified to account for market realities.

REGULATORY RISK – KEY QUESTIONS

- Do I fully understand all the regulatory requirements and implications applicable to my institution, my agents and my customers?
- Am I in full compliance with these regulations?
- Have I identified potential areas for risk of non-compliance?
- Do I have assurance that processes are adequate to ensure ongoing compliance?
- Have I established a positive and productive relationship with my regulator?

Is there an operations manual that details all business processes?

3. Operational Risk

Operational risk is inherent in any business and refers to risks associated with products, business practices, damage to physical assets, as well as the execution, delivery and process management of the service. In practice this refers to the large and diverse range of activities needed to administer the business. For the most part, operational risks are internal to the organization and can therefore be carefully managed. In terms of DFS, the critical new area of operation is the day-to-day business of supporting the channel. This can include functions touching every part of the business, such as:

- Sales operations: including agent recruitment, training, and on-going agent management
- Customer service operations: providing assistance to external users of the service (customers, agents, and others) and escalating issues that they cannot resolve
- Back office operations: such as creating and editing agent and other business accounts, trouble-shooting issues, and testing any changes to the service (usually minor operational updates)
- Finance operations: including creation of e-money and ensuring that the bank and e-money (control) account match, and providing business reports
- Technical operations: providing the hosting environment and support for the technology.

Business Processes: The key to efficient operations that minimize risk is to have high quality, efficient and effective business processes. Business processes should always add value to customers and mitigate risks. While many institutions blame technology or governance as the cause of fraud, many cases of major internal DFS fraud can be traced back to inadequate (or non-existent) business processes that allowed fraudsters to abuse the service. See page 48 for a full description of potential fraud risks.

Every operational process that is performed on a regular basis should be documented, describing what needs to be done, how to do it, and who is responsible for doing it. Business processes should also cater for exceptions, specifying what to do if something goes wrong at any point in the process and the standard path cannot be followed. Internal audits are used to ensure that business processes are adhered to by staff.

Business processes need to be reviewed and updated regularly to ensure that they are still relevant. This is particularly important in the early part of the service lifecycle. Within a few weeks of launching a service, the gap between expectation and reality for many procedures becomes obvious. It is recommended that draft business processes created prior to launch are reviewed and finalized three to four months after launch, when the operations team have experience of real-life operations. Thereafter, they should ideally be reviewed annually. If a new functionality is introduced, for example involving a new partner such as bank-to-wallet transfers, new business processes will be required to manage the new activities.

Suitable technology can be used to prevent the occurrence of many risk events, but ultimately, particularly as the technology for many DFS is not yet fully mature, the best protection from operational risk is well constructed business processes that are properly followed and updated, and which are regularly reviewed during internal audits to ensure compliance.

Internal Control: Internal control procedures are used to protect against fraud, disruptions, reputational risk, and credit risk by ensuring adherence to business processes. The internal control department conducts operational audits on the organization and its agents to ensure that correct procedures are being used in terms of transactions, account opening, KYC, and branding standards. The internal control department tests the effectiveness of such procedures and standards and makes suggestions and revisions to policies and procedures based on a continuous feedback and learning loop.

Internal Audit: Internal audits provide assurance and checking of processes and controls. The internal audit department is responsible for ensuring that financial reporting is accurate and reflective of the real state of financial affairs of the institution; that business risks are assessed and mitigated; and that controls are effective. Internal audit may conduct monthly financial audits of the institution, high risk functions and processes, as well as operational spot audits of branches and agents, ensuring proper liquidity management, recording of transactions, and to detect agent fraud and other misdemeanors.

Segregation of Duties: Segregation of duties is a procedural methodology that ensures there are adequate checks and balances in place to protect against conflicts of interest and control breakdowns. An example of segregation of duties is the accounting principle (sometimes known as "maker, checker and approver") whereby the person carrying out a transaction or process is separated from the one recording or reviewing the activity and the one approving the activity, in order to minimize errors and opportunities for fraud and mismanagement of funds. IT systems can be set up so that there is role-based access depending on the requirements for each job function. An example of role-based access is to enforce segregation of duties so that an operator can only access those functions required to perform his job. For example, customer care does not need access to the financial section where e-money is created; finance does not need access to the sales section where agent accounts are created; junior team members may have access to maker tasks, but not to checker tasks; and so on.

External Reporting: Large funders, donors, and shareholders, such as parent institutions, may require additional reporting in order to monitor performance, minimize risk of their investments, and to ensure early detection of problems, either operational or financial. Reporting is usually conducted quarterly for financial reporting and semi-annual for qualitative reporting on progress, challenges and lessons learned.

External (Financial) Audit: Most institutions, especially regulated or public institutions, are required to have external audits conducted at least once per year. An external audit is mostly focused on financial reporting of the institution and to ensure accurate posting of transactions as well as adequate depreciation and valuation of the institution's assets. It may also include further checks on controls, particularly for high risk activities and processes.

Damage to Physical Assets: Damage to physical assets can result from normal wear and tear, natural disasters, acts of terrorism, or vandalism. Risks may be magnified using DFS as physical assets are in trust to outside parties such as agents and may be in geographic locations where the institution does not have regular in-person visits. It is important that potential damage to physical assets is included as part of business continuity plans and disaster recovery plans. Potential mitigation strategies can include property insurance, back-up systems, and off-site data storage.

Execution, Delivery and Process Management: Operational risk derived from operator error in execution, delivery and process management includes risks such as data entry errors, accounting errors, lack of mandatory reporting and negligent loss of client assets. It is closely linked to technology risk and is more prevalent in DFS due to outsourcing of transaction to agents. In some regions, regulators are now implementing new guidelines to reduce this risk and protect customer funds. Mitigation of operator error risk can include "segregation of duties" between the person conducting the transaction or other activity, the person recording or reviewing it, and the person approving it; role-based access to systems; agent and staff training; monitoring; transactions in suspense accounts; monitoring suspicious transactions to flag frequent errors in the transaction sequence, or specific agents or staff that make errors frequently. Data analytics, dashboards, and algorithms can be powerful tools in mitigating operator errors if they are followed up by resolution, training, or policy enhancement that reduces the risk of continued errors.

Reconciliation and Account Variances: The risk that the actual value in trust accounts is different from the amount reflected in the e-money system, as well as the risk that off-net transactions (e.g. ATM withdrawals and bill payments) are not reconciled with internal accounts. Some variance may always occur, but high levels of variance, or those that are irreconcilable, may lead to financial losses.

EXAMPLE 3

Risk Register

Operational Risk – insufficient manuals

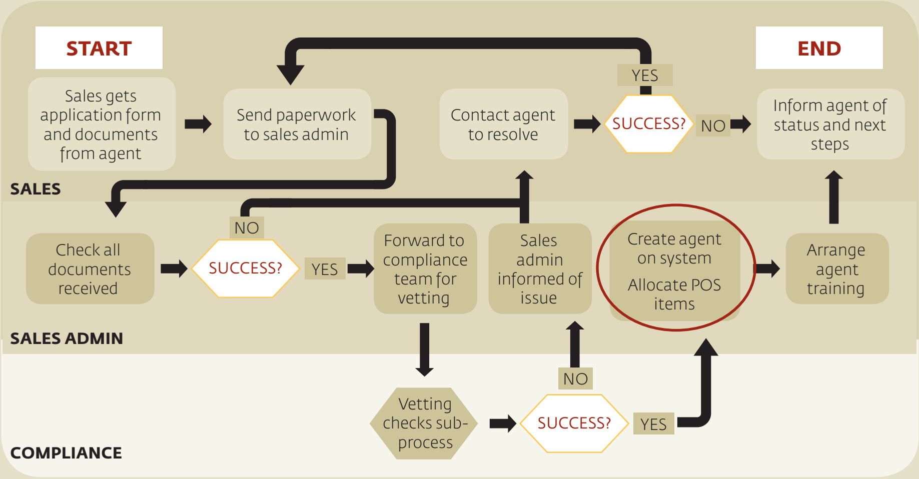
DFS Provider example:	Either an agent banking service OR an MNO that offers a mobile money wallet
Risk Category:	Operational Risk
Secondary Category:	Regulatory Risk
Name:	Lack of operational manuals and business processes
Description:	Back office inefficiency because the operating manuals are incomplete, lacking the exception processes when things do not go according to plan.
Owner:	Head of DFS
Cause:	Poor planning and implementation of operational procedures to support DFS
Effect:	Could lead to mismanagement of systems, customer accounts or funds resulting in compliance violations or loss of funds
Probability:	*2 out of 5* *Moderately low, based on knowledge of risk and development of tools, however, still a risk that not all scenarios are covered*
Impact:	3 out of 5 *Moderate impact, based on leading to reputational and financial losses, but not sufficient to cease operations*
Risk Strategy:	Treat
Treatment Strategy:	• Review operating manual against list of procedures being undertaken. Add any missing procedures, update existing procedures as required and add the exception use cases to all. Ensure that relevant departments sign off each process • Create process checklists and ensure all processes have been documented and are regularly reviewed and updated if required • Make business process maintenance a key deliverable of the operations team.
Treatment Tactical Response:	• Identify missing exception procedures. Convene a team to determine what they should be and which functions are responsible for them • Document these process exceptions • Train staff on implementation
Key Risk Indicator:	• Productivity of back office team measured by » numbers of suspense transaction resolved » or number of days transaction stay in suspense accounts » or time taken to resolve disputes • Transaction exceptions with "in progress" status • Call center issues resolution rate
Current status:	Has not occurred

Box 3
Operational Risk Case Studies

Following the success of mobile money in East Africa, as mentioned earlier, many MNOs decided that they needed to have their own mobile money service as soon as possible. Typically, little thought was given to the technical or operational requirements when they were looking for a mobile money system and they relied upon the technology vendor to understand what was required. As this was a new type of service, there were no off-the-shelf technical solutions, but many vendors, mainly software providers with successful money transfer or airtime transfer systems, were keen to fill the gap. Most of them had gained a good understanding of the user experience of both customers and agents but had no access to or comprehension of the back office system and the tasks that mobile money operators had to perform. As a result, many early systems looked good from a user perspective but did not provide the functionality or the reports needed to operate the services efficiently. The DFS industry is littered with service provider stories of their disappointment with the technology they initially bought and its inability to perform the necessary operations (despite often an inability to articulate what was expected from the technology when it was purchased).

Technology should reinforce, not replace, strong business processes that specify how a service should be operated. It is unfortunately still common for DFS providers to have either no formal business processes or incomplete procedures that have not been updated since they were written, and are rarely used. When asked for their operational business processes, they simply produce training manuals for operating the technology. For example, a simple business process for on-boarding new agents could be represented[6] by the diagram below:

Figure 4: Business processes cover the end-to-end task, not just instructions for operating the DFS system


START
END
Sales gets application form and documents from agent
Send paperwork to sales admin
Contact agent to resolve
SUCCESS?
YES
NO
Inform agent of status and next steps
SALES
Check all documents received
NO
SUCCESS?
YES
Forward to compliance team for vetting
Sales admin informed of issue
Create agent on system
Allocate POS items
Arrange agent training
SALES ADMIN
Vetting checks sub-process
NO
SUCCESS?
YES
COMPLIANCE

[6] This example is for illustrative purposes and is not a comprehensive description of the full business process described.

The diagram describes all of the tasks needed to on-board the agent, of which entering his or her details into the DFS system (highlighted in red) is only one part. In the absence of documented processes, it is easy for operators to forget some steps in the process, particularly the "exceptions" where things go wrong, for example if the agent fails some vetting checks, or if full documentation is not received. This can result in potentially good agent applications suffering delays, or inappropriate retailers being accepted as agents.

In the absence of comprehensive business processes, some essential operation tasks can be overlooked. The missing processes are often "exceptions" when things do not go according to plan. A good example is SIM recycling. Because there is a limited range of phone numbers that can be used by any MNO, if a number is not used for an extended period, typically six months, the SIM card with that number is disconnected and the number recycled and used with a new SIM card. If there is not a process to detach the DFS account from that phone number, then the new SIM card already has a live DFS account associated with its phone number. Because the new owner of that number did not set up the DFS account, they do not know the PIN code and cannot use that account; nor can they register a new DFS account against that number. MNOs recycle many thousands of numbers every month, but because this is an issue that only becomes apparent long after the DFS launch, processes to detach DFS accounts from recycled numbers are often overlooked.

In addition, the operations team needs to be able to respond quickly to new unforeseen problems. For example, there was a major issue when bill payments were first introduced in one market because during the bill payment, customers were asked to enter their utility account number as a reference. The account numbers shown on utility bills all had a space in the middle of them, but in the electricity company system there was no such space. Customers that included the space when they paid their bills had the money deducted from their wallet, but the reference could not be recognized by the utility system and their accounts were marked as overdue, and many cut off. The DFS operations team had to quickly find a way to identify customer accounts with this problem, reverse the payment to return the money to customers' wallets, and then contact the customer and explain how to make the payment successfully.

OPERATIONAL RISK – KEY QUESTIONS

- Do you have an independent board and internal audit department?
- Is there an operations manual that details all business processes that is regularly reviewed and updated?
- Are critical business processes identified and relevant controls assessed?
- Is there adequate segregation of duties?
- Is there a daily reconciliation process between the bank and e-money accounts to minimize errors and detect fraud?
- Are there regular, rigorous and adequate internal and independent external audits?

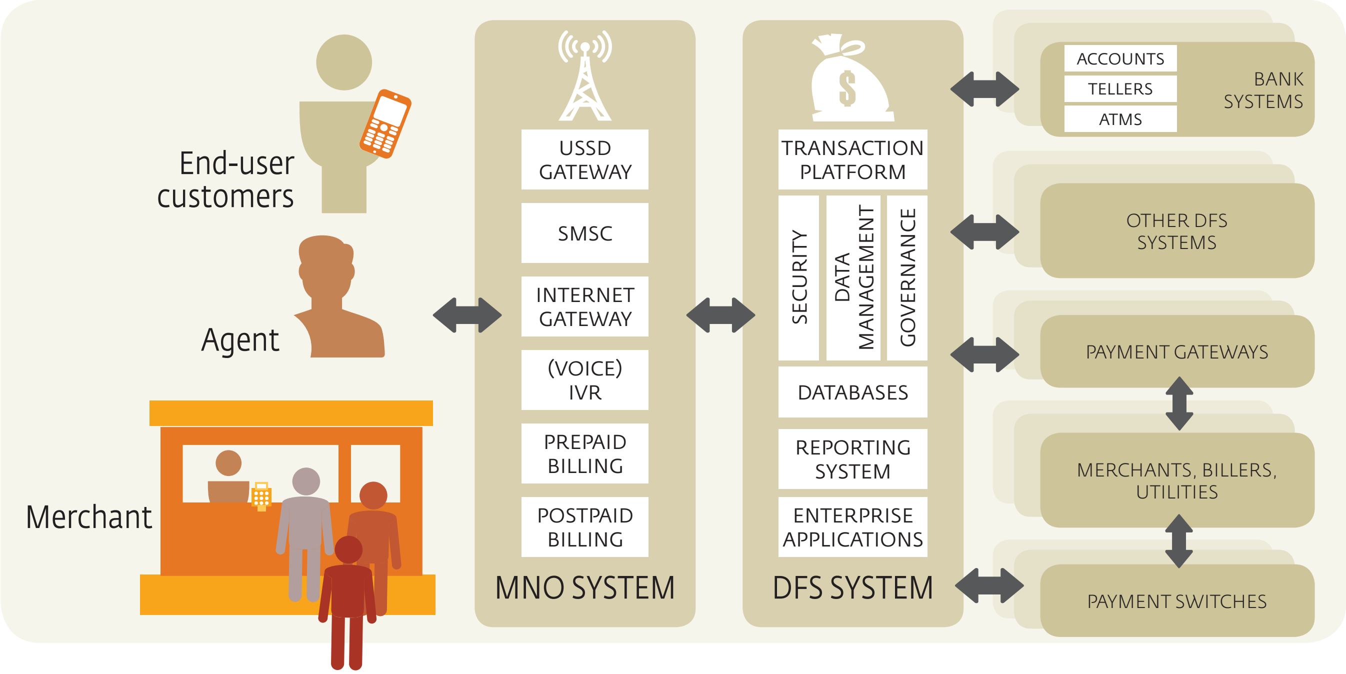
Am I able to measure the service level from an end-user perspective?

4. Technology Risk

Technology risk has several implications for providers. With the inability to conduct transactions, both agents and customers can lose confidence in the product if they cannot access their funds. This can create reputational risk and financial losses as customers and agents become inactive and competitive pressure provides them with alternative choices. Technology failure also leaves opportunities for fraudsters to take advantage of system inadequacies to conduct unauthorized transactions resulting in theft of funds. See the Fraud Risk section below for full descriptions of the types of fraud that could take place.

Technology Risk refers to technology failure that leads to the inability to transact. It is closely linked to operational risk. Transactions within a DFS travel through several communications systems and devices in order to initiate the transaction, transfer funds, and communicate confirmations with clients. The process may be exposed to potential breakdowns from a number of sources e.g. hacking, power failure, system faults etc., and any breakage in this chain leads to an inability to complete a transaction. If technology failure is persistent and severe the regulator may step in and impose penalties or revoke the license, or customers may abandon the service.

Figure 5: As DFS systems become more connected, the number of potential points of failure increases



When determining service levels provided by the technology, most technical departments focus on the quality and availability of the technology for which they are responsible. For complex multi-component DFS, this can lead to a silo mentality where each team tries to pass blame for a system failure to another partner. It is therefore important to have clear and agreed fault diagnosis, resolution, and escalation processes in place. Another potential risk in the division of responsibility is that each technical team measures the quality of service of its part of the system only, and it can be difficult to get a complete picture of the end-user experience. When entering into partner agreements to provide DFS, it is essential to determine in advance technology KPIs such as Transactions Per Second or system up time and ensure that these can be measured in full.

Software Failure: Inherent in any technical system is the potential for software issues. There are many potential causes of software failure, such as bugs, changes to seemingly unrelated systems both in-house and in partner systems, and poor update and maintenance procedures. If systems are not adequately maintained and available so that customers, merchants, and agents are unable to access their funds and transact when needed, it may result in a loss of business for the DFS provider and significant reputational damage. It is not realistic to imagine that any system can provide 100 percent availability, but service outages can be minimized by employing rigorous good practices.

Identification of potential software failures begins with identification of all systems involved in each type of transaction. There are several different systems and types of software that may be involved in a DFS implementation, including core banking systems, payment systems, switches, agent management systems, POS/ATM applications, mobile applications, biometric systems, and client relationship management software. Once identified, a risk analysis can be conducted to understand the potential vulnerabilities of the institutions' own systems and their interactions with other systems. As far as possible, providers should also understand the pressure points in their partners' systems to ensure that partners can fully provide the required service levels. At each layer, providers should have a consistent plan for training, testing, and maintenance of the software, with proactive measures to prevent and detect any potential issues that could affect service. In addition, providers must ensure that they have a clear service level agreement with their service providers and technology vendors that details not only response and resolution times for issues, but confirms the roles and responsibilities of each party.

Typically, for business critical systems, the DFS provider should specify system availability and other KPIs to ensure quality of service and then work to enforce these standards with all parties involved in the channel. System performance is strongly influenced by the scale of operations, and a commonly used KPI is the number of transactions per second that can be handled. As the business grows, it is important that there are regular meetings between technical and commercial teams to ensure that there is sufficient capacity planning to cope with growth and to support any marketing campaigns that could cause a demand spike.

Hardware Failure: Hardware failure is the inability to transact due to failure of physical devices including ATMs, POS devices, and mobile handsets, as well as back-office servers and networking components. Additionally some channels may be dependent on peripheral devices such as biometric readers, printers or card readers. Clearly the biggest risk lies with the servers that host the DFS applications. Providers need to ensure that they have a solid business continuity plan in place. This should include backup servers that can easily be utilized in a case of failure, ideally through a 'mirrored' service that ensures that the live servers are replicated in real time so that in the case of failure the backup will be immediately available. Power outages can be an issue in many emerging markets, so reserve power supplies are needed. These may be generators in large establishments like the provider offices, or as simple as solar chargers for the POS devices. In addition, there is a need for disaster recovery systems that can be brought online at short notice in case of a catastrophic failure of the main servers, such as fire, flood, or a terrorist attack. Many countries have regulation dictating the minimum distance between the main site and that of the disaster recovery system, and the maximum duration of the switch-over before the service is once again available.

Unavoidable "wear and tear" necessitates regular maintenance and updating of hardware. Many companies now operate systems in the cloud and assume that this ensures a constantly maintained and updated, distributed system in which capacity increases and disaster recovery is guaranteed. These assumptions need to be clarified in the hosting contract and regularly reconfirmed. However, using the cloud presents other potential risks. Cloud based services rely on high quality internet links, and the provider should use a minimum of two independent internet services in country with sufficient capacity and availability on different internet routing. Another risk of cloud services is security; cloud-based servers make the DFS provider dependent on the cloud provider to ensure that suitable security measures are in place and the DFS provider may need to perform an audit of the hosting sites and protocols to confirm that this is indeed the case.

Agent hardware may be supplied directly by the DFS provider, or may be procured independently by the agent. Devices are not typically covered by service level agreements, but rather through manufacturer warranties. When selecting agent devices, there should be legal agreements concerning device maintenance, repair and replacement, including liabilities, timings and costs as well as expected normal failure rates for the devices. It is important to note that hardware failure may be caused by failure of the device itself, or failure of its connection to the back-end software. It is important that the provider is able to quickly diagnose the root cause of hardware failure in order to know the type of solution to apply to maintain service.

Network Connectivity Failure: Hardware failure also includes connectivity issues, which continue to be a major challenge in developing markets, particularly in rural areas. Intermittent coverage, insufficient availability, and network downtime inhibit transactions and can result in a loss of business. Connectivity starts with the internal networks of the provider and extends to communication infrastructure that connects to third parties involved in the channel offering and to the client.

If networks are down, the user will not be able to initiate a transaction. If this is a persistent issue, it will lead to reputational risk as it affects the customer experience when customers wait for long periods of time for networks to come back on line. Since voice and SMS channels are relatively more stable and have wider availability than data networks, many providers choose to use those channels instead of data. In one example, an MFI procured POS devices with dual SIMs so that their agents could switch between them when one operator was down.

Transaction Delays: Transaction delays may be caused by the technology having insufficient capacity to deal with demand, causing queues in the system. There are multiple interconnected systems involved in DFS and a breakdown at any point in the chain could cause the transaction to delay, often leaving the customer and agent unaware of whether the transaction has completed or not. This can include delays in receipt of a confirmation SMS to the customer's device. Transaction queues can also have more significant consequences, such as the system failing to process transactions or leaving them hanging indefinitely.

Transaction Replay: Mobile operators use "transaction retry" patterns, which automatically resend transaction requests if an immediate confirmation is not received. These replays carry the risk of the user initiating duplicate transaction requests because they do not realize that the transaction was successful the first time around until after they have already made several attempts. There is also the risk that the network creates multiple messages based on a single message from the user.

Loss of Data: Data protection should be included in the providers' business continuity plans to ensure that customer data is not lost or compromised through theft, loss, neglect or insecure practices. Customer data should be stored off-site with backups.

Cyber Attacks: Cyber-attacks are security threats to the integrity of a provider's client and transactional data, as well as potential attacks of corporate espionage in order to gain access to internal process and technological strategies through hacking or malware. Financial services was the second most attacked sector in 2015[7], after healthcare. The introduction of DFS provides potential hackers additional access points in which to attack systems and data and can create new risks.

A variety of factors are driving exposure to cybersecurity threats. The interplay between advances in technology, changes in business models, and changes in how firms and their customers use technology creates vulnerabilities in information technology systems. For example, web-based activities can create opportunities for attackers to disrupt or gain access to corporate and customer information. Similarly, employees and customers are using mobile devices to access information from financial institutions, which creates a variety of new avenues for attack. The landscape of threat actors includes cybercriminals whose objective may be to steal money or information for commercial gain, nation states that may acquire information to advance national objectives, and hacktivists whose objectives may be to disrupt and embarrass an entity. Attackers, and the tools available to them, are increasingly sophisticated. Insiders, too, can pose significant threats.

Cyber-attacks are often carried out in four stages: *infiltration* where the attacker gains first access; *propagation* where the attacker expands access through back doors or password mining; *aggregation* where the attacker collects records and data; and *exfiltration* when the data is exported. Most defense is focused on the infiltration stage, but since attackers are often most skilled in this area successful defense should be included at all stages. To manage the risk of cyber-attacks, providers can work with auditors to develop threat models where breach points are mapped and mitigation strategies developed. In addition, providers can protect themselves by using cloud services that are likely more secure than proprietary hosting, or purchase cyber-attack insurance to protect against losses from financial and data loss or legal expenses.

Institutions should build their cyber capabilities keeping the following points in mind:

- A sound governance framework with strong leadership is essential. Board- and senior-level engagement on cybersecurity issues is critical to the success of cybersecurity programs.
- Risk assessments serve as foundational tools for institutions to understand the cybersecurity risks they face across the range of the firm's activities and assets—no matter what the firm's size or business model.
- Technical controls, a central component in a firm's cybersecurity program, are highly contingent on individual situations.
- Institutions should develop, implement, and test incident response plans. Key elements of such plans include containment and mitigation, eradication and recovery, investigation, notification, and customer communication.
- Institutions typically use vendors for services that provide the vendor with access to sensitive firm or client information or access to firm systems. They should manage cybersecurity risk exposures that arise from these relationships by exercising strong due diligence across the lifecycle of vendor relationships.
- Well-trained staff represent an important defense against cyber-attacks. Even well-intentioned staff can become inadvertent vectors for successful cyber-attacks, for example through the unintentional downloading of malware. Effective training helps reduce the likelihood that such attacks will be successful.
- Institutions should take advantage of intelligence-sharing opportunities to protect themselves from cyber threats. There are significant opportunities to engage in collaborative self-defense through such sharing with other financial institutions and regulators.

[7] Auditing Cyber Security in an Unsecured World, The Institute of Internal Auditors, 2015

EXAMPLE 4

Risk Register

Technology Risk – network connectivity failure

DFS Provider example:	Either an agent banking service that uses mobile technology as its primary means of transacting OR an MNO that offers a mobile money wallet
Risk Category:	Technology Risk
Secondary Category:	Reputational Risk
Name:	Network connectivity failure
Description:	Customer cannot perform transactions through mobile application or at an agent due to: • Mobile phone service is not available • The provider's system is experiencing temporary system downtime
Owner:	Head of IT
Cause:	Poor performance of vendor technology, insufficient capacity in DFS system, inadequate MNO service
Effect:	Transactions cannot be performed, resulting in loss of revenue and poor customer experience
Probability:	2 out of 5 *Moderately low based on diligent selection of vendors and service level agreements*
Impact:	3 out of 5 *Moderate in the short term as the customer is likely to try again until successful. However, persistent problems will lead to reputational and financial loss*
Risk Strategy:	Treat
Treatment Strategy:	• Test the mobile operator's ability to deliver messages at the required service level on a periodic basis • Test end-to-end transaction process time taken and success rate periodically • Install performance monitors to show the system traffic and raise alarm if it approaches peak TPS • All transactions defined with clear completion boundaries, thus allowing for clear rollback procedures in the event of incomplete transactions • Service level agreements with system providers that have detailed strategies for enforcement • System upgrades • Use USSD enabled POS as a fall back to mobile data (3G) to reduce reliance on data connectivity
Treatment Tactical Response:	• Invoke penalties from service level agreements with vendors • Develop offline transaction modes
Key Risk Indicator:	• Transaction success rate (of transaction requests reaching the system) • Sufficient capacity to cope with peak transaction rate • Calls to customer services about failed transactions
Current status:	Occurred and controlled

Box 4
Technology Risk Case Studies

A) When M-PESA was launched in Kenya, a bespoke system was commissioned from a software developer. There was little hard evidence on which to base the volume forecast that in turn would provide the basis for the system capacity requirements. It was felt that an optimistic but realistic forecast was that by the end of the first year there would be around a third of a million active customers, each transacting about three times per month. The system was built with the capacity to service this requirement plus a reasonable margin of error. Adding capacity to enable processing larger numbers of transactions, larger databases to hold more customer and transaction records, and all the supporting architecture "just in case" would be very expensive and unjustified, so the system was built to meet the expected demand. Of course, M-PESA's success was beyond any expectation and within three months of launch it was clear that the forecast was far too low. The technology was struggling to keep up with the unforeseen huge number of transactions being submitted. A task force was set up to find ways to increase capacity quickly but even so, customers started to experience transaction delays and occasional system breakdowns which required manual intervention to process transactions by a large team of customer service representatives. For several months the technology team was constantly "running to stay still", finding ways to add capacity that was full by the time it was deployed. In parallel they were building longer-term solutions to the intrinsic architectural constraints. Whilst the capacity issues were eventually resolved, the incremental cost of constant improvements to the under-sized launch technology were extremely significant.

B) Fidelity is a tier one bank in Ghana with close to one million customers, 80 branches, 110 ATMs and 1000 banking agents. To address the financial exclusion of 70 percent of Ghanaians, the bank established a Financial Inclusion Unit to pioneer agent banking in 2013. The flagship product is the Smart Account, an entry level card-based product using agents for basic services normally provided at bank branches.

To support the Smart Account business, a new stand-alone system was purchased. Agent banking was a young business sector at the time with many technology providers creating new systems, and few services had a proven track record. Fidelity decided to test the waters by selecting an add-on technology platform separate from its core banking system. Deploying new technology is always a source of risk. As the agent business was new to Ghana and Fidelity Bank, it took *the bank some time to assess the full needs of the market and as a result it could not upfront build in the flexibility the system needed to allow for changes as the project progressed.*

"You need to thoroughly investigate and anticipate your requirements, and state and restate. Otherwise, the supplier may give you a solution for today and not tomorrow."

~Dr. William Derban

The Smart Account was launched in July 2013 with very high expectations. By the end of the first six months, Fidelity had opened over 55,000 accounts. The agent numbers grew rapidly, as well as the volume of transactions. However, as the number of transactions grew, Fidelity begun to experience a number of challenges. Some related to the fact that this was a new service in the country, and staff and agents had no other examples of bank agents to compare to or learn from. Secondly, the technical system seemed inflexible and unable to cope with the increased demands on it from a fast evolving market. Unplanned downtime has improved significantly, but remains a big issue. Coupled with unacceptable transaction failure rates (agent POS devices began to show failure rates of around 20 percent and problems were encountered in linking the core banking and Smart Account agent systems), it forces the team to focus on constant fire-fighting instead of business development, especially as numbers of Smart Accounts ramped up (to approximately 300,000).

Even though the Smart Account and the agent banking channel have grown exponentially since inception, the high targets set by Fidelity Bank are yet to be achieved. With more advances in agent management systems in the past few years, Fidelity is investing in improving its technology platform and to move its agent banking and Smart Account business onto the same platform as the main bank.

Technology can be a major source of risk, especially when you are a pioneer as in the case of Fidelity Bank. Today, with over two years' experience and still the only commercial bank with bank agents in Ghana, Fidelity is optimistic that its technology risk has been greatly reduced as it improves on its current technology platform.

TECHNOLOGY RISK – KEY QUESTIONS

- Do I have service level agreements with my system provider to ensure software uptime?
- Do I have service level agreements as well as fault diagnosis and repair procedures in place with my partners?
- Am I able to measure the service level from an end-user perspective?
- Is my software adequately communicating with devices to minimize transaction failures?
- Are third party providers and vendors effective and adequate in their security protocols and risk management approaches?
- Is access to corporate IT assets restricted and only granted based on an established role-based access framework?
- Do I have any mechanism in place to prevent loss or leakage of sensitive information (confidential information, intellectual property, personally identifiable information) from the organization?

Are my trust accounts adequately diversified?

5. Financial Risk

Financial risk is one of the most impactful risks related to DFS. While all risks discussed in this paper can have direct or indirect financial losses, there are specific risks related to the financial management of a DFS provider as described below.

Liquidity risk: Liquidity risk is the risk that the institution is unable to meet its cash flow obligations and becomes insolvent. Transactional patterns such as average deposit amounts, inflows, outflows, and durations should be monitored closely after the launch of DFS as customer behavior may be affected by having convenient access to funds and this may change the asset/ liability profile of the financial institution.

Credit risk: Credit risk is the risk that clients do not repay their loans and either do not have sufficient collateral or the institution is unable to collect on it. In this case, the institution is still responsible to its deposit holders and must find alternative ways to repay them in case loans turn bad.

Interest Rate risk: The risk of the interest rates on borrowed funds increasing, while at the same time, being unable to increase the interest rate charged to customers due to long term loan rates being locked in. In this case, the institution would be paying more in interest to creditors than they are earning by lending it, creating significant financial losses.

Foreign Exchange risk: Foreign exchange losses can be incurred when trading currency, or by having a mismatch of currencies in which loans and deposits are denominated. Book values of debt obligations can grow substantially through adverse fluctuations in currency, resulting in losses. Forex risk can also be an issue if the organization's income is generated in a different country to where its costs are incurred.

Concentration risk: Concentration risk refers to overexposure to a particular counterparty (credit) or sector. If there is a concentration of funds held at any one particular bank, the institution is at risk of excessive loss of client funds should the bank become insolvent. Placing funds at multiple banks will help mitigate this risk, although it creates additional administration. Similarly, over-reliance on a particular customer segment may risk large amounts of revenue should customer preferences change such that large amounts of deposits are withdrawn.

EXAMPLE 5

Risk Register

Financial Risk – foreign exchange exposure

DFS Provider example:	Any DFS provider that incurs a high proportion of its costs in a different currency to the one in which they receive income. For example a PSP operating in several markets from a central head office.
Risk Category:	Financial Risk
Secondary Category:	Strategic Risk
Name:	Foreign Exchange Risk
Description:	The risk that financial losses are incurred due to fluctuations in foreign exchange rates.
Owner:	Head of Finance
Cause:	External causes such as economic performance and monetary policy of local governments
Effect:	Leads to real or book losses if liabilities are in foreign currency and it appreciates
Probability:	2 out of 5 *Moderately low probability due to stable currency exchange rates over last ten years*
Impact:	4 out of 5 *Moderately high impact if fluctuation is severe enough*
Risk Strategy:	Transfer
Treatment Strategy:	• Source local borrowings or foreign borrowings in local currency to the fullest extent possible • Negotiate contracts with vendors and providers in currency of borrowings • Transfer remaining risk that cannot be avoided
Treatment Tactical Response:	• Purchase currency swaps for exposed risk
Key Risk Indicator:	• Foreign exchange rate
Current status:	Has not occurred

Box 5

Financial Risk Case Studies

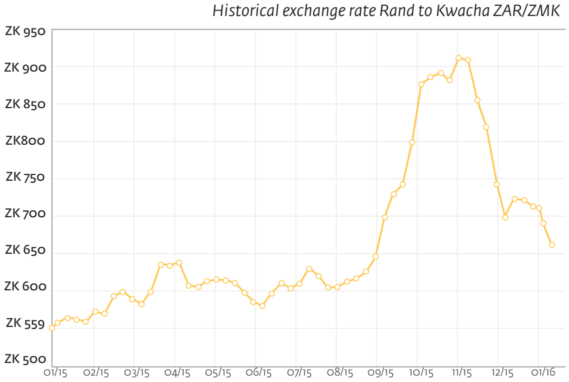
Zoona is an independent financial services provider that offers over-the-counter financial services via agent networks in Zambia, and more recently in Malawi. Its 1,400 active agents provide mainly domestic remittance services to 1.3 million individual customers, with over 90 percent of transactions coming from its longer established Zambian business.

Zoona has a centralized support office, which handles technical support, customer care, and certain other corporate functions for all operating entities. Only a relatively small team is therefore needed in the countries of operation to provide sales support, setup and any other operational functions that must take place locally. This centralization is intended to provide economies of scale as the business expands into new markets. Cloud-based technology is used, reducing the technical overhead and allowing rapid expansion when required. Thus the staff level is low, with around 60 percent of the workforce based in the support office and the rest in the local markets. Nevertheless, the biggest cost to the business is staff related costs.

This geographical separation of operations from the markets mean that Zoona has a currency mismatch in that it earns revenue in local currency but has a large proportion of its expenses in South African Rand and US dollar. When the exchange rates were relatively stable, this was not a problem. However, the majority of its revenue currently comes from Zambia, and the Kwacha dropped in value versus the Rand by almost 60 percent in the latter part of 2015.[8]

[8] *(Forex chart from http://fx-rate.net/ZAR/ZMK/)*

Fortunately the exchange rate appears to be returning to previous levels. Currency fluctuations are obviously beyond the control of Zoona, but the risk is so high that steps are needed to mitigate this risk. Apart from normal treasury hedging techniques, management is taking the approach of diversifying into a number of different markets to help mitigate the impact of changes in one currency.



Historical exchange rate Rand to Kwacha ZAR/ZMK

FINANCIAL RISK – KEY QUESTIONS

- Do I have sufficient funding and cash to meet obligations and buffer for unexpected cash flows?
- Do I have credit risk policies in place including credit risk assessments and KPIs for portfolio monitoring?
- Am I aging my portfolio at risk and creating loan loss reserves as per my regulatory requirements?
- Is my trust account(s) adequately diversified and covered by deposit insurance?
- Is my foreign currency hedged?
- Are internal back-office processes, reconciliations and controls adequately designed, verified and monitored regularly?

> *Are there any foreseeable political threats?*

6. Political Risk

Political risk is the possibility that political decisions, events, or conditions, will significantly affect the profitability of a business or the expected value of a given economic action. Political risks are faced by institutions as a result inter alia of civil unrest, terrorism, war, corruption, slowed or retracting economic growth, or unsuitable economic conditions following fiscal or monetary policy changes set by the government. Events caused by political risk have impacts on operational risk, in particular business disruption and should be included in business continuity plans.

Political risks are beyond the control of the organizations and customers affected by them, but can have a serious impact on the business. Whilst they cannot be prevented, in some cases they can be predicted, such as known elections, and contingencies set in place in case the risks materialize, as happened to two IFC partners discussed in Box 6 below.

EXAMPLE 6

Risk Register

Political Risk – sudden system disruptions

DFS Provider example:	Any DFS provider as all are reliant upon agents and communications technology.
Risk Category:	Political Risk
Secondary Category:	Reputational risk
Name:	Inability to access account or conduct transactions.
Description:	Post-election violence, civil unrest, war or terrorist activity disrupt normal business operations, by directly closing the business, or closing an essential partner function such as the mobile network, or the retailers that operate as agents
Owner:	Head of Risk
Cause:	Political instability, elections, war, terrorist attack and/or outside disruption
Effect:	Customers cannot access accounts due to loss of connectivity or inability for agents to operate business as usual
Probability:	*1 out of 5* *Very low given history or civil peace in local market*
Impact:	*3 out of 5* *Moderate impact based on potential for business disruption*
Risk Strategy:	Tolerate
Treatment Strategy:	• Develop service disruption plan for agents, staff and/or branches
Treatment Tactical Response:	• Invoke service disruption plan for agents and staff
Key Risk Indicator:	• PAR • Service availability (uptime) • Agent activity • Customer activity
Current status:	Has not occurred

Box 6

Political Risk Case Studies

A) FINCA DRC is a microfinance institution founded in 2003 that launched an agent banking service in 2011 to expand its footprint beyond its 18 branches. Its 548 agents form the largest agent banking network in the Democratic Republic of Congo, where only 4 percent of a population of 75 million has an account with a formal financial institution. FINCA now holds a quarter of a million customer accounts that can be used for savings and loans. More than half of FINCA's business is transacted via agents using biometric POS terminals. Transaction details are communicated from the agent POS device by mobile data network to a switch which links to the FINCA servers via a secure internet connection.

In response to demonstrations against proposed extensions to the presidential term in January 2015, the DRC government disabled all internet, voice and mobile data services. MNOs and Internet service providers complained of losing millions of dollars of business during the shutdown. The POS devices of FINCA agents became inoperable, and customers were unable to access their accounts. As a result, customers could not repay outstanding loan obligations to FINCA. The FINCA portfolio at risk rating increased, and did not fall back to its previous level in the months after the disruption. As PAR is a key performance indicator for assessing portfolio quality, the few days of disruption in early 2015 led to long term negative performance and significant financial losses. The mobile (voice) network was restored within two to three days, and the internet was restored for corporates, including financial institutions, after ten days, but the impact was still being felt long afterwards

Political unrest is expected to continue in the DRC, and FINCA is understandably very concerned about this, making plans to minimize business impact. Political factors remain beyond its control, and the consequences of a prolonged period without network connectivity could be profound.

B) LAPO Microfinance Bank is a Nigerian microfinance bank operating in 26 states, currently providing 1.3 million customers with microfinance services. It is in the process of creating an agent banking service to supplement its regional branches.

LAPO has significant assets in the north east of Nigeria where there have been several serious terrorist attacks in recent years.This has caused branches to be closed at short notice, and in one instance staff and customers were trapped inside *a branch for several hours during a nearby incident. In financial terms, the uncertainty caused by civil unrest also has an impact on the quality of the loan assets, impacting its ability to grow the portfolio.*

LAPO is launching its agent network in 2016, and the disruption caused by terrorist groups is likely to continue. LAPO has instigated a number of measures to mitigate the risks, including provision of training and a staff manual giving guidance on what to do in case of being in the vicinity of a terrorism situation. The agent model is particularly vulnerable to political disturbances given that LAPO relies on its relationships with its agents to manage business disruption. Mitigation techniques should be integrated into the agent training and management systems.

POLITICAL RISK – KEY QUESTIONS

- Are there any foreseeable political threats, or imminent events that might create a political threat? If so, am I prepared?
- Do I have contingency in place to manage the implications of an outage due to political events?
- What is my communication plan to customers, partners and investors in the event of political risk affecting my business?

Have we developed detective controls for fraud?

7. Fraud Risk

Fraud is a notorious risk for DFS and the cause of much concern to DFS providers. Fraud risk is multi-faceted and relates to several other risks. Operational and technology risk can cause fraud risk, and fraud can lead to financial risk. Fraud is also a significant driver of reputational risk. Large cases of fraud in mobile money have been reported over the last few years that have caused financial damages of millions of dollars. These have been due to customer, agent, and employee fraud from creating ghost accounts and conducting fraudulent transactions. Funds have been stolen from providers, agents, and customers. Fraud can have a large impact on the reputation of an institution, and the industry as a whole. If funds are stolen from customer accounts at the fault of the provider, providers must ensure that funds are returned to customers immediately. The process of preventing fraud includes conducting assessments to understand where fraud could be detected and prevented, determining risk appetite and establishing effective controls.

Fraud can generally be defined as either major fraud involving very large sums and usually perpetrated against the financial institution, often by staff; and minor fraud involving agents or customers as victims or perpetrators and smaller sums of money.

There are many reasons why people commit fraud, but a common model to bring a number of these together is The Fraud Triangle[9]. The premise is that fraud is likely to result from a combination of three general factors: Pressure (or motivation to commit fraud); Opportunity (typically because of poor systems or processes); and Rationalization (typically that they will not be caught).

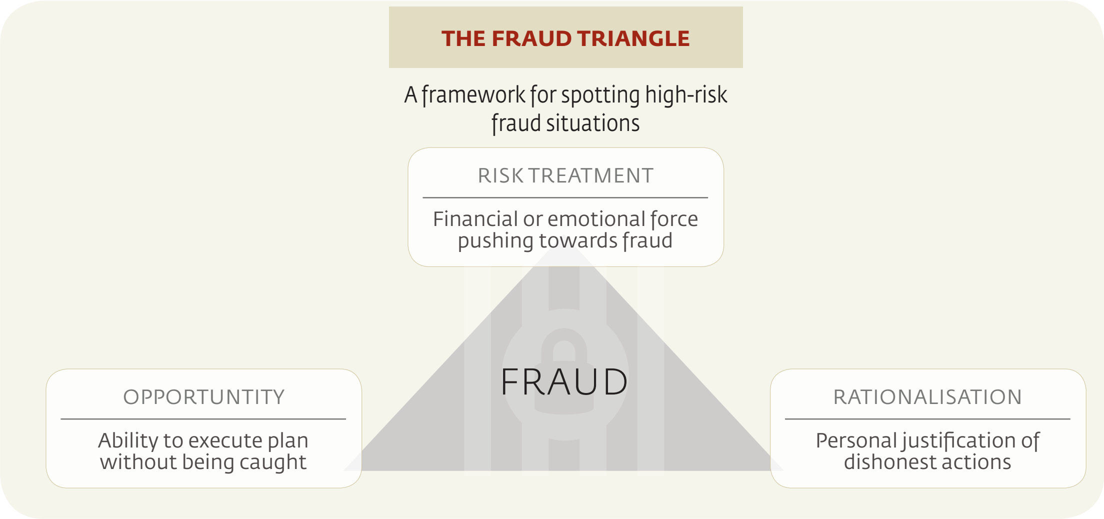
One of the most effective ways to prevent fraud is to decrease the opportunity for fraud, by having excellent fraud prevention and detection technology and procedures. This reinforces the need for fraud risk management.

The most common types of DFS-related fraud are defined in the MicroSave publication *Fraud in Mobile Financial Services* (2012)[10] and have been summarized below by source of fraud.

[9] http://www.cimaglobal.com/Documents/ImportedDocuments/cid_techguide_fraud_risk_management_feb09.pdf.pdf

[10] MicroSave Fraud in Mobile Financial Services, Mudiri, 2012

Figure 6: The Fraud Triangle: framework for spotting high risk fraud situations


THE FRAUD TRIANGLE
A framework for spotting high-risk fraud situations
RISK TREATMENT
Financial or emotional force pushing towards fraud
FRAUD
OPPORTUNTITY
Ability to execute plan without being caught
RATIONALISATION
Personal justification of dishonest actions

Customer Fraud

CUSTOMERS DEFRAUDING AGENTS

- Counterfeit currency: the risk that customers deposit counterfeit currency at an unknowing agent in exchange for electronic value, and then withdraw legitimate currency from another agent.
- Unauthorized access of agents' transaction tools: customers access agent POS devices to conduct fraudulent transactions.
- Fraud on agent web channel: Customers access agent web channel without authorization and conduct fraudulent transactions.
- Voucher fraud: fake vouchers are made to represent genuine vouchers from NGOs or government and given to agents in exchange for cash or electronic value.

CUSTOMERS DEFRAUDING CUSTOMERS

- Unauthorized PIN access: customers gain access to other customer's PIN numbers and conduct unauthorized transactions.
- Identity theft: customers use IDs of other customers to gain access to accounts.
- Phishing, SMS spoofing, fake SMS: fraudulent customers send fake SMS to agents either from their own handsets or generated from computers. The SMS looks genuine to the recipient.

Agent Fraud

AGENTS DEFRAUDING CUSTOMERS

- Unauthorized access to customer PINs: agents gain access to customer PIN numbers and conduct fraudulent transactions.
- Imposition of unauthorized customer charges: agents charge customers fees for transactions above and beyond the list price and fraudulently keep the fees instead of remitting to the provider.
- Split withdrawals: customers request a withdrawal from the agent, and the agent splits the withdrawal in two or more transactions in order to collect more cash out commissions from the customers.

AGENTS DEFRAUDING PROVIDERS

- Split deposits: customers request a deposit from the agent, and the agent splits the deposit in two or more transactions in order to collect more cash in commissions from the provider.
- Direct deposits: agents directly deposit funds from a customer into another customer's account instead of cashing in, and then send a transfer funds request in order to avoid the fee.
- Registration of customers with fake details: agents sign up customers that do not provide accurate KYC information.
- Registration of non-existent customers: agents sign up ghost-accounts in order to receive the registration commission.
- Registration of individuals as businesses: agents sign up customers as a business account in order to receive the higher commission.
- Impersonation of provider status: an unauthorized agent acts as an authorized agent to conduct fraudulent transactions.
- Money laundering on platform: agents knowingly conduct transactions for customers that are for the purposes of money laundering in order to receive commission.

AGENT EMPLOYEES DEFRAUDING AGENTS

- Theft of funds: agent employee steals funds from the cash float at the agent.
- Underreporting of cash balances: agent employee misrepresents the cash float balance at the agent.

FRAUD BY MASTER AGENTS

- Unauthorized withdrawals from agent accounts: master agents abuse access to agent accounts and withdraw funds.
- Illegal deductions from commission earned by agents: master agents charges excess commission splitting fees to the agent.

Business Partner Driven Fraud

EMPLOYEES DEFRAUDING BUSINESSES

- Employees link wrong mobile numbers to bank accounts: employees link their own mobile or a corroborator's mobile number to a bank account in order to have illegal access to the account.
- Illegal reversal of customer payments to the business: employees reverse payments conducted by customers and keep the cash.
- Illegal transfers from business accounts: employees conduct fraudulent transactions transferring funds from business accounts to fraudulent accounts.

System Administration Fraud

- Abuse of passwords: employees use access to passwords to conduct fraudulent transactions.
- Creation of fake/non-existent users: employees create fake accounts in order to conduct fraudulent transactions.
- Individual users with multiple rights: employees are given access to multiple levels within systems and are abused to conduct fraudulent transactions.
- Weak passwords/transaction PIN: employee passwords are hacked due to weak password settings.

Provider Fraud

CONTACT CENTER AND OPERATIONAL SUPPORT FRAUD

- Unauthorized access of customer payment records: employees abuse access to customer records.
- Illegal transfer of funds from customer accounts: employees conduct fraudulent transactions.
- Unauthorized SIM swaps: call center staff change customer PIN numbers.
- Unauthorized access to co-workers' system access rights: call center staff gain access to co-workers' access rights in order to conduct fraudulent transactions.

Sales and Channel Staff Fraud

- Bribery: sales team bribes agents and/or customers or request unauthorized payments.
- Unauthorized access of agent transactional data: sales staff use agent data to conduct fraudulent transactions.

EXAMPLE 7

Risk Register

Fraud Risk – split deposits

DFS Provider example:	MNO that offers a mobile money wallet and uses agents to cash in for a fixed (or stepped) commission fee
Risk Category:	Fraud Risk
Secondary Category:	Agent Management Risk
Name:	Split deposits
Description:	Agents force customers to split deposits into a number of smaller transactions in order to generate higher commissions at the cost of the provider.
Owner:	Head of DFS
Cause:	Commission structures incentivize misbehavior of agents.
Effect:	Provider is forced to pay higher commissions to agent than originally intended which can severely impact net revenue.
Probability:	*1 out of 5* *Moderately low based on strict policies and controls*
Impact:	*1 out of 5* *Very low based on largest potential loss is transaction fee*
Risk Strategy:	Tolerate
Treatment Strategy:	• Use data analytics tools to flag suspicious transactions such as multiple transactions to or from the same account at the same agent within a 24 hour period • Develop a comprehensive due diligence process for the recruitment of agents to minimize recruitment of agents with poor reputation or those likely to commit fraud • Carry out mystery shopping activities to identify agents trying to split transactions and practice good agent management by using remedial action • Education of agents by including split transaction warnings in agent training materials • Call center for customers to report suspicious activity
Treatment Tactical Response:	• Agent retraining • Enforcement of penalties for agent mismanagement and closure of agents
Key Risk Indicator:	• Suspicious transaction reports
Current status:	Occurred and controlled

Box 7
Fraud Risk Case Studies

One of the most reported large scale frauds experienced by a DFS was due to poor operational practices. The service was one of the early DFS deployments in Africa and it soon became successful. Because of this success in a highly competitive market, the service providers focus was on increasing numbers of customers and transactions and as a consequence, little attention was paid to the many warning signs that all was not well. Within a few months of launch, the employees tasked with daily reconciliation, ensuring that the e-money issued matched the money in the bank account, were reporting large discrepancies. These warnings were ignored by management. For nearly two years a number of employees created "counterfeit" e-money that was not covered by "real" money, and became increasingly creative in finding ways to cash it out, for example via complicit agents or by creating bogus customer accounts. This was possible due to a lack of operational controls that allowed the perpetrators to abuse the system with impunity. Operators could create their own logins, with some individuals having multiple user IDs to confuse any audit trail. There was no segregation of duties enforced to prevent operators from processing bogus transactions, and no suspicious behavior monitoring to identify potential fraud. New staff were not formally trained on operating the complex back office system and thus could not recognize inappropriate behavior by their colleagues, or correct any issues. Possibly the worst omission was that there were no procedures in place to investigate any issues that were reported, so the various fraudulent activities lasted for several years before being uncovered.

There are many reported instances of small scale agent fraud. One of the most common is splitting large transactions into many smaller transactions. For example "split withdrawals" are where a customer wishes to cash out a specified amount and instead of doing a single transaction, the agent performs multiple smaller withdrawals and *earns a fixed amount on each. This is possible because most services pay the agent a fixed amount per withdrawal rather than a percentage, making it possible to earn the same commission multiple times instead of just once.*

Another way for agents to scam the provider is to register customers who have come in for an airtime top up for the mobile money service without their knowledge or consent in order to earn a commission. An added sophistication on this scam occasionally occurs when an agent registers a genuine customer and then offers to demonstrate how the service works by doing a deposit, immediately followed by a withdrawal, using the new customer's phone. The agent earns commission on both the cash in and cash out despite no real exchange of money having happened.

FRAUD RISK – KEY QUESTIONS

- Have you determined your level of acceptable financial losses due to fraud?
- Have you identified the key areas for potential fraud risk for your institution?
- Have you developed preventative and detective controls for fraud?
- Are you actively monitoring and reviewing your fraud risk management strategy?

> *Do you provide enough training for agents and distributors?*

8. Agent Management Risk

The introduction of agents to act on behalf of financial services providers presents many benefits in cost, geographical reach, and scale, but also introduces new risks. The management and supervision of agents is imperative to a well-functioning service that protects customers. The use of agents can trigger operational, technological, legal, reputational, and fraud risk, which are covered in other sections. In addition, there are risks directly associated with agent management:

Agent Density: Customers use agents to access their mobile financial service, especially for cash in and cash out, and require close proximity to an agent in order to conduct transactions. However, providing the right number of agents to meet customer demand is always a challenge to any DFS. Insufficient agents can refer either to a lack of nearby agents, or lack of capacity of the nearby agent to meet customer demand, resulting in long queues or liquidity problems (see below).

On the other hand, too many agents can also be a risk because the customers are diluted amongst them so that no agent has the critical mass of customers needed to earn sufficient commission to offset the cost of e-money and cash float management. In these circumstances, the agents often fail to maintain float and are thus unable to serve customers. Infrequent usage of the DFS can result in agents forgetting how to offer the service or to forget their PIN so that they cannot serve customers, even if they have liquidity.

Insufficient Liquidity: Agents require sufficient cash on hand and electronic value to manage customer's transaction requests for cash in and cash out on a day-to-day basis. To meet these needs, agents typically use cash float from their existing businesses; travel frequently to a branch or another agent to exchange cash and e-float; or, for busy agents, utilize a relationship with a liquidity manager, such as a super-agent, from whom they can access fast and frequent turnaround of cash and float. In some cases, liquidity facilities may be offered by the financial service provider or a third party in the form of initial capital infusion or a short term overdraft to offset shortfalls in liquidity. Sufficient liquidity management processes and facilities are required to ensure that agents are satisfied and not inconvenienced, and for customers to trust that there are funds available immediately upon request.

Theft of Cash Float: An agent's business operations may be put at risk from excessive deposits. The cash may be stolen, and this is especially the risk if the agent develops a reputation for holding large amounts of cash. Liquidity managers should offer pick-up and drop-off services to mitigate this risk.

Teller Errors: Agents and their tellers may make key stroke errors in entering transactions or counting errors in cash management that will result in a float being unreconciled and sustaining losses either to the agent or to the customer. Teller errors also include the risk of losing or damaging paper records that may put the agent and provider at risk of regulatory non-compliance.

Poor Training: Training of agents is typically standardized and rooted in the provider's policies and procedures to comply with regulatory guidelines. Training policies include the training content, the required frequency and timing of the agent training, and the required trainer qualifications. Agent training should be thorough and include refresher courses to mitigate risks of errors and to provide a consistent customer experience across all agents. It is essential that those serving customers at agent locations are trained, not just the agent service owner, and this can be a challenge. It is common for badly trained agents to claim that the service is not working, rather than admit that they don't know how to use it. Customers that have a poor first experience at an agent are often discouraged from using the service again, and may even be discouraged from using DFS at all.

Customer Service Mismanagement: Agents are the first line of customer service for DFS providers. Included in the training on policies and procedures should be mechanisms for agents to handle customer complaints and inquiries such as basic troubleshooting, provision of call center numbers, and the logging of complaints for relaying to the agent manager. Agent mishandling of customer service can impact providers through loss of customers, inactive accounts, and reputational risk.

Poor Agent Selection: Agent selection policies typically include minimum suitability criteria (based on regulatory requirements and the provider's assessment of required capacity). Poor agent selection may lead to inactive agents, reputational risk, regulatory risk and financial losses for the provider. Agents should be well trained on the requirements for maintaining their agent status, monitored frequently, and closed if not meeting the minimum criteria.

Inadequate Branding and Marketing: Branding and marketing materials should be standardized and included in the policies and procedures for agent management. Branding and marketing materials should be provided by the financial service provider and can include signage, brochures or other collateral. A consistent user experience is important to reduce the risk of client inactivity and reputational risk. There should be sufficient supply of marketing materials to support customers in their early use of the service.

Whilst the regulator takes a hands-off approach to agents in many markets, some countries may require a provider's use of agents to be approved by regulators and in some, each agent must be individually licensed. Supervision of agents may be conducted by regulators; however, even if that is the case, providers should also be conducting oversight themselves. Agent supervision by providers including data analytics and in-person visits reduces the opportunities for risk in the DFS operations, such as fraud risk, reputational risk, regulatory risk and strategic risk, as well as improving the likelihood of success by increasing activity rates of agents and customers.

EXAMPLE 8

Risk Register

Agent Management Risk – liquidity constraints

DFS Provider example:	Any DFS provider that relies on agents having a store of value (or e-money) in their accounts to serve customer deposits. For example an MNO that offers a mobile money wallet.
Risk Category:	Agent Management Risk
Secondary Category:	Reputational Risk
Name:	Lack of agent liquidity
Description:	Customer cannot perform cash in transaction because the agent does not have sufficient e-money
Owner:	Head of DFS
Cause:	Agent is capital constrained or chooses not to invest in DFS operations, or has no convenient mechanism to quickly access e-money
Effect:	Customer cannot cash in because there is no e-money available, resulting in poor customer experience
Probability:	3 out of 5 *Moderate probability based on difficulty of controlling agent liquidity levels*
Impact:	2 out of 5 *Moderately low impact based on customers' ability to return later or visit another agent. If service is early in life cycle, or problem is persistent, impact will be higher.*
Risk Strategy:	Treat
Treatment Strategy:	• Use of agents and super-agents for liquidity • Call center logs • Process to alert agents when their e-money float is low • Control the roll out of agents to ensure that there is both sufficient geographical coverage, and that each agent has sufficient customers to support his business • Process to identify when agents are consistently failing to meet their liquidity requirements, and mitigation procedures • Pre-fund agent capital requirements through loans or lending institution partnerships • Mystery shopping and good agent management
Treatment Tactical Response:	• Increase capital requirements and agent due diligence for new agent sign-up • Re-evaluate commission structure to ensure sufficient incentives in place.
Key Risk Indicator:	Agent e-money balances
Current status:	Occurred and mitigated

Box 8

Agent Risk Case Studies

According to the GSMA,[11] on average 51.4 percent of DFS agents are active, or around half of the agents recruited to offer DFS to customers are actually doing so. In some markets, the inactivity level is much higher. This means that customers may walk into a fully merchandised DFS agent to perform a transaction, only to be told that the agent is not operational. Worse still, in an attempt to save face, these agents often tell customers that they cannot be served "because the DFS is not working today" which undermines the service by making it seem unreliable and unsafe. A bad agent experience can damage the DFS reputation and put potential customers off using it, especially if it happens early in the customers' exposure to the service. Common causes of agent inactivity are either that the agents do not know how to use the service, or they have forgotten their PIN codes, or they have run out of e-money float.

Agents need to have a supply of e-money float to send to customers wishing to deposit money; and they need cash to give to customers wishing to make a withdrawal. Even among active agents, liquidity issues are common, especially in rural areas far from the nearest bank where cash can be deposited to replenish the e-money supply. If customers cannot easily access the money in their accounts, or if they think the intended recipient of the money will have trouble cashing out, they are put off using the service. This creates a downward spiral, as agents do not bother to maintain their e-money float regularly if they are not experiencing customer demand, so more customers have a bad agent experience and stop (or never start) using the DFS. Because of this, successful DFS providers have a range of strategies to ensure that their agents have access to several ways of managing float, such as enabling aggregators and super-dealers to assist agents, and providing merchant payments by DFS to continually top up the agents e-money holding.

[11] GSMA state of the industry report: mobile money 2015. Inactive agents are defined as not having served a customer in the previous month.

AGENT MANAGEMENT RISK – KEY QUESTIONS

- Do you have concrete agent agreements that cover all of your risks and abide by local regulation?
- Do you have a comprehensive training program for agents and distributors?
- Do you have a range of contingency plans to facilitate liquidity management?
- Do you have feedback processes in place to identify and resolve agent performance issues?

Are partners assessed for reputational risk?

9. Reputational Risk

Reputational risk refers to the risk of losses from damage to the image of a provider, partner, or stakeholder, leading to a reduction of trust from clients and agents. Losses may occur in reduced revenue and shareholder value, as well as increased operating costs or legal liability. Reputational risk is not a direct risk, but is a result of other risk-related problems, such as many of those discussed throughout this handbook. However, by its nature, the consequences can be severe and long lasting. The risks that are most likely to result in reputational damage are technology failure causing an inability to transact, lack of transparency in policies and pricing, fraud, poor customer experience, lack of agent liquidity, and high prices.

The best way to protect the business from reputational risk is to have a strong risk management function to prevent those risks most likely to affect the service or the company's reputation. Risk prevention includes minimizing opportunities for fraud or those risks caused by poor customer experience such as failed transactions, lack of connectivity and liquidity, or poor agent experience. Preventing reputational risk can be achieved by focusing on the customer experience and building trust. Creating a good customer experience can be achieved by ensuring customers can access their funds when and where they need them, as well as creating avenues for customer recourse such as encouraging and supporting agents to provide first level customer service, operating well-managed call centers to solve customer complaints and inquiries, and returning customer funds in any cases of fraud. Reputational risk is also an effect of partnership risk if partners fail to meet clients' expectations. The provider should be prepared to address issues and maintain customer relationships, even if the event was the fault of the partner.

For those risks that cannot be avoided, a mitigation strategy is used. A key component of a mitigation strategy is a public relations strategy that has contingency to manage negative press, either reactively or proactively, depending on what the situation requires. Most organizations already have a PR strategy for damage limitation, and the DFS business should be included with key personnel briefed about the service so that they can react quickly to reputational threats. As DFS can be quite complex, it is advisable to also have a nominated person from the DFS team to liaise with the public relations manager to ensure that the correct messages are being delivered.

Whilst press briefings are the first step towards mitigating reputational risk, it is also advisable to communicate directly with agents, merchants and any other DFS partners to reassure them about the situation. In addition, customer services should be briefed and provided with agreed statements that can be communicated to concerned customers. It is also important to communicate internally to appraise staff and reassure them.

EXAMPLE 9

Risk Register

Reputational Risk – transaction failures

DFS Provider example:	For example an MFI that offers agent banking
Risk Category:	Reputational Risk
Secondary Category:	Technology Risk
Name:	Poor customer experience caused by technology risk
Description:	Agents cannot perform a transaction when requested by customers because the service is not available for several hours
Owner:	Head of DFS
Cause:	The DFS is suffering an unplanned technical outage
Effect:	The service gets a reputation for being unreliable. Agents are embarrassed. Customers are not confident that they can access their money. Over time they stop using the service
Probability:	2 out of 5 *Moderately low due to strong technology risk mitigation*
Impact:	2 out of 5 *Moderately low based on unlikelihood of losing all customers*
Risk Strategy:	Treat
Treatment Strategy:	• Prevention of risk event that would lead to reputational risk • Strong SLA with the technology provider, based on robust technology • Incident resolution process and escalation matrix in place • Well-resourced customer care department • Customer feedback channels through agents, call centers, social media, email, branches, or other channel
Treatment Tactical Response:	• Communications plan to alert the business to the outage, and then for agents and other partners to be advised of the issue and its expected resolution time • Procedure in place to manage press enquiries about the incident • Customer care advised of how to handle calls from customers and agents
Key Risk Indicator:	Short and long term KPIs (did the incident affect the expected performance of the business?)
Current status:	Has not occurred

Box 9

Reputational Risk Case Studies

A) A successful DFS provider discovered that it had been defrauded of a significant amount by corrupt employees. The police was called in and the suspects charged. Because of this, it seemed unlikely that it could "hush it up" and avoid a scandal. After some debate it decided to go public in the press, explaining what had happened, that the issue had been stopped, and that none of its customers had suffered as a result. The public reaction was, as might be expected, that customers favored the competitors because of security concerns and a resulting drop in sales. It is not known what the drop in sales would have been if it had kept silent and the fraud had been revealed by the media in headline news. On balance the DFS provider now believes it should have kept quiet and hoped for the best.

B) A major African MNO was one of the successful early DFS providers. A couple of years after launch it experienced internal fraud that was reported in the national press. A scandal ensued. The MNO admits to the damage this scandal caused its business:

"Definitely the damage was far beyond mobile money in our country…It was beyond the MNO and touched the whole mobile money space. Reputational damage was manifold."

For a while, the reputational damage extended beyond DFS to its core telecoms business. In addition, the entire DFS sector in this market was affected; its major competitor confirmed that this incident also impacted its DFS sales as the loss of consumer confidence shrunk the whole market.

REPUTATIONAL RISK – KEY QUESTIONS

- Do I understand the financial value of reputation, or the potential cost of losing it?
- Do I consider reputational risk with strategic risk?
- Do I have clear standards linked to the preservation of reputation and integrity?
- Are partners assessed for reputational risk?
- Do I have a comprehensive communications and public relations plan to proactively address rumours or concerns with my service?
- Do I have a comprehensive customer support line for customers and agents?
- Are there guarantees in place to protect customer and agent funds?

Do you share expected outcomes and KPIs with your partners?

10. Partnership Risk

DFS partnerships are often necessary, and valuable in terms of providing expanded services to clients and improving operating efficiency. In some cases partnerships are required by regulations. In all cases, some level of cooperation and partnership is required as the banks rely on MNO networks for connectivity and the MNOs rely on banks to hold funds in trust. Effective partnerships are equally rewarding relationships that have unique value propositions for each party and provide an improved experience for the customer.

The Partnership for Financial Inclusion program published a study in 2014[12] outlining lessons learned from partnerships in DFS. It found that there were four key factors for success in DFS partnerships:

- Deficiencies in the partnerships from either one or more of the partners not playing a role that is key to their success, or one or more of the partners playing a role they are ill-equipped or unmotivated to play;
- DFS partnerships must enable the partners to generate value for their respective companies;
- Partnership roles in a DFS implementation must be aligned with competitive and comparative advantage and motivation;
- The lack of level playing fields in regulatory environments leads to suboptimal partnership arrangements.

Business partnership risk can include the breakdown of relationships with operational and strategic partners including distributors, master agents, vendors, technology providers, implementation partners, and donors. It can also be a source of reputational risk.

Bank and MNO Partnerships: As the world of DFS expands to include new products such as algorithm-based lending and bank-to-wallet integrations, bank and MNO partnerships are becoming more and more common. In many markets across Sub-Saharan Africa, bank-to-wallet integrations are now common place allowing customers to move funds between bank accounts and mobile wallets and to cash in and out using either bank or MNO agents. The fluidity of funds creates a better user experience for the customer, but hybrid models involving banks and MNOs are also at the highest risk of partnership breakdown. The two institutions try to work together to build a client-facing single product, and the question of who owns the customer often becomes a challenging discussion. If the partnership was to break down, both the product and client retention could be at risk. Institutions need to develop

[12] Partnerships in Mobile Financial Services: Factors for Success, IFC, 2014

a mitigation strategy for retaining the customer in the event this may happen. Mitigation strategies may include pro-active management of customer relationships through customer service, marketing and branding campaigns, as well as outlining customer ownership agreements within the partnership agreements and including clauses around things like exclusivity and non-compete issues. In some markets, banks are the smaller, less dominant DFS partner and may find it difficult to negotiate a level playing field with MNOs. It may be decided that they are better off playing the background role of holding accounts and loans, while the MNO manages the client-facing relationships.

Agent Distributors: When utilizing complex agent network structures in a business model for DFS, the performance of the agents can be largely dependent on the ability of the master agent to manage them. This typically encompasses training, provision of liquidity, marketing materials and incentives. The relationship between the provider and the master agent plays a key role, and the breakdown of this relationship may result in a disruption to customer experience. Partnership agreements with agent distributers should cover all levels of services, and clearly state expectations and remuneration to reduce partnership risk inherent in the relationship. They should also contain clear rules on how the ending of a partnership will be conducted to minimize impact on the customer or the business.

Vendors: Vendors play a large part in a DFS rollout. The risk of technology failure has a large impact on the customer experience and the partnership the provider holds with its vendors can affect the risk of transaction failures and service delays.

Technical Integrations: Most services are dependent on technical interfaces with third parties. The first and foremost requirement for technical integration is for connectivity. DFS have an inherent requirement to use data or voice networks to offer services using technology. This includes the use of mobile network access, including SMS, USSD, and 3G services.

Beyond the basic requirements around connectivity, as DFS services mature, they are increasingly integrating with other technologies, often via Application Program Interfaces. These include integration with core banking systems to allow funds to be transferred between DFS accounts and conventional bank and MFI accounts; integration with billers such as utilities, either directly or via payment switches; integration with various POS devices; and integration with money transfer organizations to facilitate international remittances. Interoperability between DFS is also starting to happen, either bilaterally or via switches.

Wherever there is a technical integration, there is a dependency on the partner service, and the integration itself is a potential point of failure. It is therefore essential that the quality of service of the partner organization is well understood before the partnership is confirmed. Poor quality of a partner is often blamed on the DFS provider. For example, if the payment switch is over-stretched the customer may need to attempt a transaction several times before a bill is paid, and this will typically be seen as a fault of the DFS. Underpinning all technical partnerships there must be a clear understanding of the service levels achievable by the partner, and an agreed expected (average) performance. Partners should be subject to penalties for consistent under-performance against these service levels. An important point often overlooked is the need to define exactly what is meant by service level and how it will be measured.

Crucially, there needs to be agreement about how incidents will be managed. When a technical incident involving two or more technologies occurs, the biggest issue can be to determine where the fault lies, with everyone claiming that another party's technology is to blame. This may be happening in a high-pressure situation if the fault is serious, so it is important to have pre-agreed procedures where all parties work together, as far as is reasonable, to identify and resolve the problem. There must also be escalation processes in place for incidents that are not possible to resolve using standard procedures.

EXAMPLE 10

Risk Register

Partnership Risk – service unavailability

DFS Provider example:	A bank offering agent banking with POS and customer mobile access provided by partner MNO connectivity
Risk Category:	Partnership Risk
Secondary Category:	Reputational Risk
Name:	Relationship difficulties between the owners of the service – leading to service outage
Description:	Significant relationship difficulty within the provider consortium results in service unavailability for customers.
Owner:	Head of DFS
Cause:	Inability of the partner to meet the increasing capacity requirements of the DFS provider as the business has grown faster than expected
Effect:	Service unavailability for customers and agents, and customers cannot access accounts.
Probability:	2 out of 5 *Moderately low based on partnership agreements and well-structured commercial arrangements*
Impact:	5 out of 5 *Very high impact based on complete dependency on partner for delivery of service*
Risk Strategy:	Transfer
Treatment Strategy:	• Services levels detailed in the partner contract • Monthly technical reviews with partners, including expected volumes, to ensure capacity planning ahead of the demand curve • Ensuring that the partner is sufficiently incentivized to keep the service running and grows with it.
Treatment Tactical Response:	• Legal action against partner for failing to provide service • Wherever possible, qualify a secondary provider to work in parallel or on standby.
Key Risk Indicator:	• System uptime • Performance vs KPIs
Current status:	Has not occurred

Box 10

Partnership Risk Case Studies

A) The Kopo Kopo business was originally founded in Kenya in 2012 to exploit the potential for M-PESA to be used for in-store (merchant) payments for goods and services. Safaricom, the company providing M-PESA, had launched "Lipa na M-PESA" (Pay by M-PESA) to consumers a year or two earlier, so the capability existed, but few merchants accepted it and usage was very low. Kopo Kopo formed a partnership with Safaricom to provide a merchant service to increase the number of retailers accepting Lipa na M-PESA and thus drive usage by consumers. The service is free to customers but merchants pay a small percentage of the transaction value as a fee that is split between Kopo Kopo and Safaricom.

Kopo Kopo recruited merchants by providing them with transaction data, business intelligence, and fast access to funds via web and android applications, as well as bulk payment and bulk SMS capabilities. In addition it took on the task of intermediating in disputes. By late 2015, Kopo Kopo had recruited 4,000 active merchants focused on specific retail channels such as catering, hairdressers, agro-dealers, and service stations. Due to this growth, Safaricom saw the opportunity to manage this business in-house and is now competing directly with Kopo Kopo to recruit new merchants. Safaricom has the advantages of scale, reputation, and offering a cheaper service as it charges just its share of the transaction fee. It has proven very successful. Anticipating the risk of a change in relationship from partner to competitor, Kopo Kopo sought to diversify in two directions:

- *To remain competitive in the Kenyan market, it has developed a popular merchant cash advance service offering funds based on a credit rating that is constantly updated based upon the merchants historical performance via Lipa na M-PESA. (This initiative is not without financial risk, but no issues had arisen at the time of writing.) By late 2015 it was earning more from its cash advances in Kenya than from its core business.*
- *By leveraging its existing investment in merchant acquirer software for Lipa na M-PESA, it has white-labeled it for use by other institutions outside of Kenya. The software will be sold on a licensing fee basis and Kopo Kopo has entered into commercial agreements with several providers. The product is due to launch in 2016 in Ghana, Uganda, and Zimbabwe, and will provide an additional revenue stream provided the service support does not exceed expectations.*

Kopo Kopo's preparedness for the inevitable emergence of its partner as a competitor has been a major factor in its business' survival in a very competitive market.

B) A major (non-telco) DFS provider suffered from fraud perpetrated by one of its partners. It contracted with the three largest MNOs in the country to use their communication *networks, specifically the SMS and USSD channels, and could provide the mobile money service to any customer or agent with a SIM card from any one of them. A number of agents started to report the same issue; their e-money float was disappearing. Over the course of two weeks this grew from one agent per day to three or four, each reporting losses of several hundred dollars. By examining the transaction statements of the affected agents around the time of the frauds, and then following sequences of transactions and accounts involved, it determined the means by which the fraud was being perpetrated.*

It noticed that all the affected agents were using agent phones connected to the same MNO, and this provided the essential clue. The fraud involved an employee in a technical role at the MNO with access to the SIM card management systems. The fraudsters had developed a scam whereby the agent PIN was harvested and the SIM card was temporarily swapped whilst the funds were withdrawn from the account. As soon as this scam was diagnosed, the MNO partner was contacted and the issue explained. Presumably the MNO tightened up its SIM swap procedures because the scam stopped within 24 hours and has never been repeated.

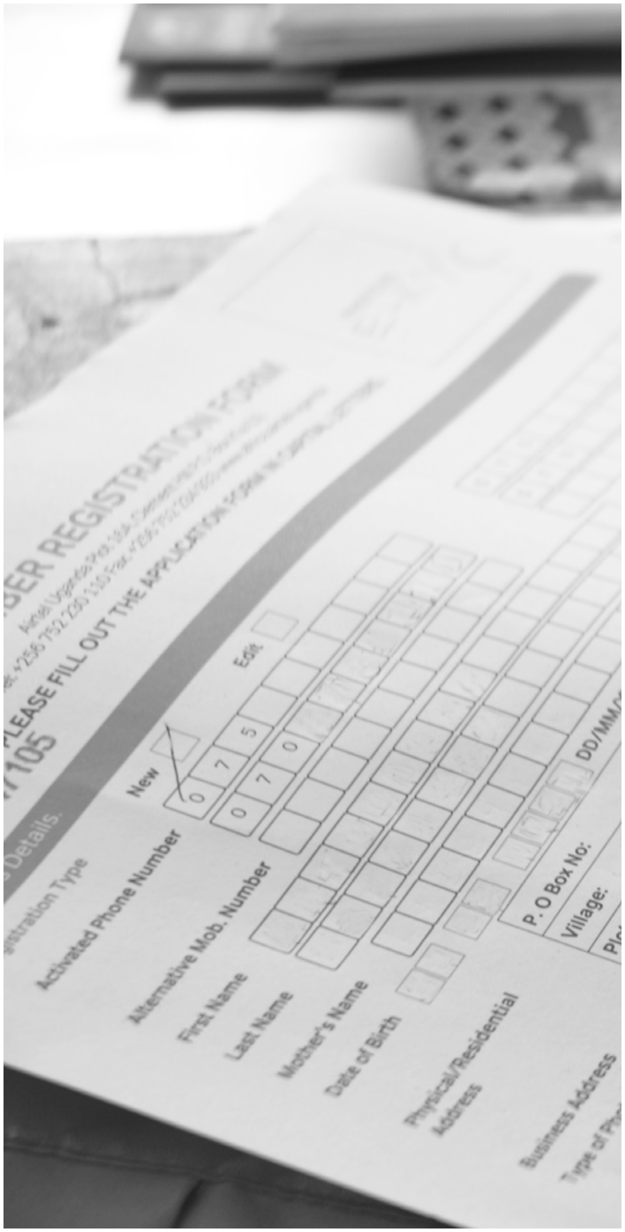
PARTNERSHIP RISK – KEY QUESTIONS

- Do you have a contract or MOU with your partner that includes protections and contingency plans?
- Do you have service level agreements with you master agents and distributors?
- Do you share expected outcomes and KPIs with your partners?
- Do you have realistic, measurable technical service levels agreed with your partners?
- Is there an agreed technical escalation process to resolve incidents?

Summary

The ten risk categories described above are broad categories used to describe DFS risk. A full list including also a number of sub-categories can be found in the risk database on page 95. As the DFS industry evolves many more potential risks will start to unfold and the task to identify, understand and mitigate risks will be a continuous one.

Now that a broad understanding has been established in Part I, and the most common currently known potential risks have been identified in Part II, institutions can move to developing risk management frameworks. Part III provides a step-by-step instruction on how to set up and implement a framework.



Customer Form
FIRST NAME*
KATUSIIME
LAST NAME*
EDVINAH
GENDER*
Box No:
Village:
Plot/Street Name & No:
DD/MM/YYYY
Type of Photo ID
Nationality
Recommendation from village chairperson/LC
Voter Registration Card
Employee ID/Letter from company wit
Passport (Compulsory for Forei
Kin Details:
Contact details:

03_

Part III

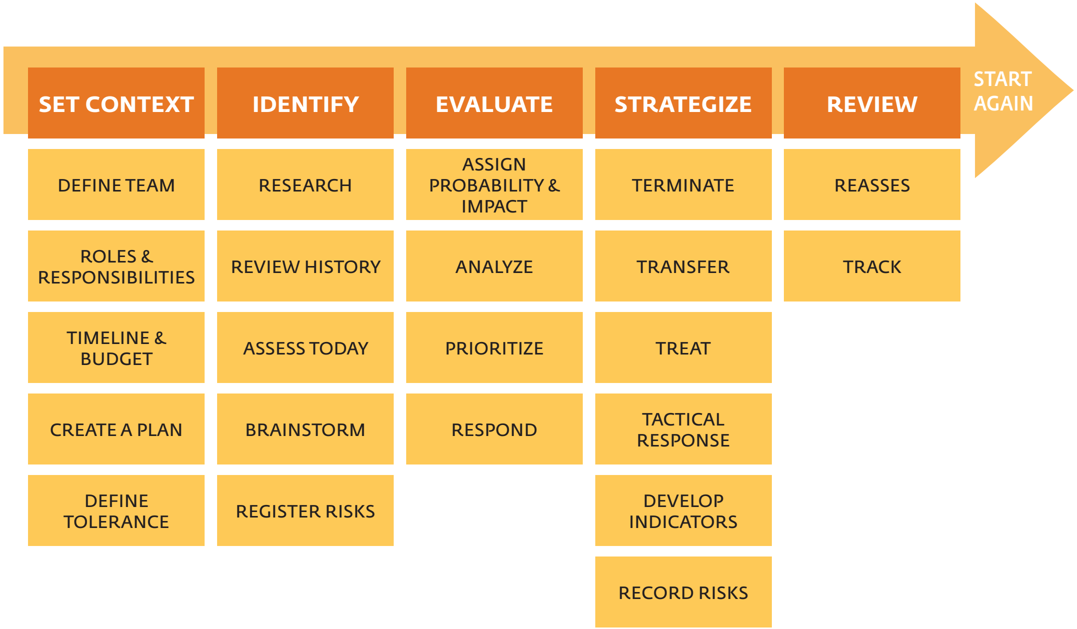
Risk Management Framework Applied

In the previous part of the handbook, we describe and illustrate the key risks in DFS implementation. In this part, we will take the concepts of the risk management framework described in Part I, and take the reader through a step by step process of the risk management cycle. It begins with Establishing Context, moves to Risk Identification, Evaluation, and Risk Strategy Development, and then concludes with Monitoring and Review.

There are several literature sources on the process of implementing a risk management framework. The GSMA has also published a risk management toolkit that uses an excel-based format to guide MNOs on mobile money risks[13]. This handbook is loosely based on the ISO 31000 business industry standards for risk management. It has been adapted and contextualized for DFS-specific risk management. The process begins with defining the project team and setting objectives and acceptable risk levels. Next, all possible risks are identified and articulated. Evaluation of the risks is done either through qualitative or quantitative methods to assess the probability and potential impact of the risk. The evaluation allows institutions to prioritize risks and to identify which risks can be tolerated, transferred, terminated, or require the development of a treatment strategy (covered in Section 4). Lastly, the framework is implemented and periodic reviews take place, going back to the planning and identification stage in order to ensure that it is always timely and an accurate reflection of the risks faced. Using the ISO 31000 Risk Assessment Process described in Part 1, there are five sections to developing risk management frameworks, as shown in figure 7.

[13] Risk Management Toolkit, GSMA & Consult Hyperion, 2015 (http://www.gsma.com/mobilefordevelopment/managing-risk-in-mobile-money-a-new-comprehensive-risk-toolkit)

Figure 7: Risk Assessment Process



SET CONTEXT	IDENTIFY	EVALUATE	STRATEGIZE	REVIEW
DEFINE TEAM	RESEARCH	ASSIGN PROBABILITY & IMPACT	TERMINATE	REASSES
ROLES & RESPONSIBILITIES	REVIEW HISTORY	ANALYZE	TRANSFER	TRACK
TIMELINE & BUDGET	ASSESS TODAY	PRIORITIZE	TREAT	
CREATE A PLAN	BRAINSTORM	RESPOND	TACTICAL RESPONSE	
DEFINE TOLERANCE	REGISTER RISKS		DEVELOP INDICATORS	
			RECORD RISKS	

START AGAIN

The sections that follow describe the activities and areas to focus in each of the steps of the diagram above.

Box 11
Creating a Risk Management Unit

Whilst many larger organizations have some kind of risk management support at group level, Tigo Pesa Tanzania is one of very few local operating companies with a dedicated in-country DFS risk management team tasked to prevent, detect, and mitigate any potential risks. The risk management team was set up in 2012, two years after the launch of Tigo Pesa, with the appointment of a DFS Finance and Risk Manager, reporting to both the head of division and to the Millicom group chief financial officer of DFS. Since then the team has grown to five people who perform a number of roles to protect the business:

***Processes and Controls** – responsible for ensuring that business processes are available for all Tigo Pesa activities, and that these are reviewed regularly and updated whenever necessary. Also controls access to log onto the Tigo Pesa systems.*

***Fraud Avoidance** – these activities are split into two types: internal fraud and customer facing fraud. Potential internal fraud is controlled by a combination of business procedures; data analysis to uncover any unusual activity; and monitoring of staff interaction with the systems to identify suspicious behavior. The majority of activity is in detecting and mitigating customer facing fraud. For example, there was an increasing incidence of customers sending money to wrong numbers and the recipients fraudulently claiming that the money was theirs. By championing the development of a new function to confirm the recipient name during transactions, the team managed to reduce this type of fraud by an impressive 60 percent.*

***Platform Integrity and Project Assurance** – any changes to the technology, whether a minor adjustment or a major new piece of functionality, has to be assessed and approved by the risk team. It takes a hands-on approach to any changes and is involved from the start of the development process.*

***Compliance with regulations** – it is the team's responsibility to provide specified reports and any other information requested by the central bank, and to assess and implement any changes to reporting or business operations required when regulations change. One team member acts as the anti-money laundering reporting officer.*

The risk management team is subject to regular peer reviews by DFS managers from other members of the group; internal audit by Millicom group; and external audit by Ernst & Young.

Section 1: Set Context

The objective of the risk management planning process is to develop the overall risk management strategy for the DFS and to decide how it will be executed and how it will be integrated in the overall DFS implementation plan. The planning process begins with the creation of a team, which then develops the timeline, costs, and outline of the risk management plan, methodology, and the process and templates that will be used in the development of the risk management framework.

Step 1: Define risk team

The team will be made up of various staff and stakeholders that will be responsible for the success of the DFS, and will also provide contrasting and complementary backgrounds in order to ensure that the risk management framework covers a comprehensive list and analysis of potential risks and the associated mitigation strategies. The team should comprise members of risk management, DFS channel management, sales and marketing, IT, finance, internal control and compliance departments, management, as well as external experts, consultants, or facilitators.

***Table 1:** Example of Risk Team*

Name	Title	Department	Contact Details
	Risk Manager	Agent Banking/Mobile Money	
	Head of Agent Banking/Mobile Money	Agent Banking/Mobile Money	
	Distribution Manager	Agent Banking/Mobile Money	
	Product Manager	Agent Banking/Mobile Money	
	Head of IT	IT	
	Marketing Manager	Marketing	
	Call Centre Manager	Customer Care	
	Regulatory Officer	Compliance	
	Finance Manager	Finance	
	Fraud Investigation Officer	Finance	

Step 2: Define roles and responsibilities

The multi-disciplinary project team is primarily responsible for assembling the risk management assessment and framework. The team will be led by a risk manager, who should ideally also be included in risk assessment and management of other projects to ensure cohesive risk management across the organization. The roles of each team member should be clearly defined and articulated up front in the planning process and recorded in the project plan.

The risk manager's responsibilities include:

- Solicit support from senior management for the risk management framework
- Determine acceptable levels of risk, in consultation with stakeholders
- Develop and approve the risk management plan
- Promote the risk management process
- Facilitate communication
- Approve risk responses when necessary
- Regularly report risk status to management and key stakeholders

Table 2: Example of Risk Team Roles & Responsibilities

Name	Title	Lead or Support
	Risk Manager	Lead
	Head of Agent Banking/Mobile Money	Lead
	Distribution Manager	Support
	Product Manager	Support
	Head of IT	Support
	Marketing Manager	Support
	Call Centre Manager	Support
	Regulatory Officer	Support
	Finance Manager	Support
	Fraud Investigation Officer	Support

Step 3: Define timeline and budget for development

The timeline for the risk management framework will be decided on by the planning team and will include start and end dates for each phase, key milestones and deliverables. Timelines should also include agreed on intervals for re-evaluation of the risk management framework.

It may be necessary to allocate a budget for the development of the risk management framework if it is expected that activities include external data collection, contracting consultants and facilitators, or off-site meeting costs. Budgets may also include contingency funds for potential losses based on the quantitative analysis in the risk assessment phase.

Table 3: Example of Risk Framework Timeline & Budget

Name	Start Date	End Date	Estimated Budget
Risk Identification	Week 1	Week 8	
Publication Review	Week 1	Week 1	
Historical Review	Week 2	Week 2	
Current Assessment	Week 3	Week 6	$15,000 for external consultant for technical advisory
Brainstorming	Week 7	Week 8	$6,000 for facilitator
Risk Evaluation	Week 9	Week 12	
Assign probability	Week 9	Week 10	$10,000 for external consultant for technical advisory
Assign impact	Week 9	Week 10	$10,000 for external consultant for technical advisory
Risk prioritization	Week 10	Week 10	$10,000 for external consultant for technical advisory
Risk Strategy Development	Week 11	Week 12	
Develop risk treatment strategy	Week 11	Week 12	$10,000 for external consultant for technical advisory
Develop risk tactical response	Week 11	Week 12	$10,000 for external consultant for technical advisory
Define KRIs	Week 11	Week 12	$10,000 for external consultant for technical advisory
Risk Framework Management Review	Week 13	Week 14	$10,000 for external consultant for technical advisory
Framework Review	Every 6 months		

Step 4: Create a plan

Planning the development of the risk management framework will include developing processes, outlines, methodologies, definitions, and templates approved by all members of the risk team.

Process: Describes the process that will be used to carry out the risk management framework development and how it will be integrated into the overall DFS business.

Outline: During the planning process, the planning team will develop an outline of the risk management framework. See page 93 for a checklist for developing a risk management framework.

Methodology: The methodology described in the plan outline will identify means by which to accomplish the qualitative and quantitative risk assessment, evaluation and analysis, risk ranking, and registering in the risk register with associated treatments. The outline of the methodology will also describe the means through which the organization will decide whether to terminate the risk, treat the risk, tolerate the risk, or transfer the risk.

Definitions: The definitions described in the risk management framework will be a glossary of terms for the team to work under common definitions of the risks.

Templates: The outline will include agreed on templates that will be used throughout the risk management framework development. Templates should include the risk register as described below, templates for brainstorming sessions for risk identification, risk analysis, and risk evaluation. The risk management framework template will also be included in the risk management plan outline.

Step 5: Establish Risk Tolerance Levels

During the planning process, the risk team will establish the risk tolerance levels of the institution, both in terms of quantitative levels of losses, as well as qualitative levels of tolerance. Quantitative values of potential losses can be estimated for most risks identified through the risk assessment process described below. The risk team will establish the level of risk tolerance, such that any risk identified with a potential loss above the threshold will be required to be avoided or transferred or if below the lower threshold, then the risk will be accepted. For example, an institution may decide that any risk with a potential impact of less than $10,000 will be accepted, between $10,000 and $100,000 will be mitigated and above $100,000 will be avoided or transferred.

Financial losses due to fraud should have some level of acceptance, as implementing risk policies to completely eradicate losses would be more expensive than accepting some levels of fraud. Once agreed upon, the acceptable level of fraud losses should be budgeted and included in forecasts and used as a Key Risk Indicator to measure performance. The industry benchmark for manageable fraud losses is seven basis points of total transaction volumes, or 0.07 percent.

The qualitative ranking described below can also be used to set risk tolerance levels such as those risks identified with a qualitative score of 1 – 5: Accept Risk, 6 – 12: Control Risk and 13 – 25: Avoid or Transfer. There may be other qualitative risk tolerance policies that the institution may wish to institute such as zero tolerance for illegal activities or regulatory violations.

Section 2: Identify Risks

The process of risk identification aims to determine all knowable risks to the DFS. However, as it is impossible to identify every potential risk, an iterative process should be used to conduct re-assessments on a periodic basis. Risk identification should be done as early as possible in the development of the DFS in order to allow for the maximum time possible for development of the risk responses. However, the earlier the identification process is done, the less certainty the organization will have about the expected probability and impact of the risk. The risk identification process can include different methodologies for identification and should include a full spectrum of risks to a DFS as outlined above.

Box 12
Customer-centric Risk Management

The greatest risk to any business strategy is that customers do not adopt the service in the numbers anticipated. Such problems are often associated with poor product design or due to a mismatch between customer and agent locations. Customers also seldom close an account. They simply withdraw their funds. This business risk needs to be understood through appropriate customer engagements, often managed by the call center or through periodic customer interviews that identifies the reasons why customers are not using the service, and added to the risk register findings.

Step 1: Research and review industry resources

It is recommended to begin by reviewing publications to identify risks that are applicable and resonate with your institution. There is a wide variety of resources available that are specific to different institution types or to specific DFS risks, such as:

- Risk Management Toolkit, GSMA & Consult Hyperion, 2015 (http://www.gsma.com/mobilefordevelopment/managing-risk-in-mobile-money-a-new-comprehensive-risk-toolkit)
- MMU Managing the Risk of Fraud in Mobile Money, GSMA, 2012 (http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/10/2012_MMU_Managing-the-risk-of-fraud-in-mobile-money.pdf)
- Mobile Financial Services Risk Matrix, USAID and Booz Allen Hamilton, 2010 (http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/06
- /mobilefinancialservicesriskmatrix100723.pdf)
- Bank Agents: Risk Management, Mitigation, and Supervision, CGAP, 2011 (http://www.cgap.org/publications/bank-agents-risk-management-mitigation-and-supervision)
- Digital Financial Services Risk Assessment For Microfinance Institutions, A Pocket Guide, AFI, 2014 (https://lextonblog.files.wordpress.com/2014/09/dfs_risk_guide_sept_2014_final.pdf)
- Mobile Financial Services Technology Risks, AFI, 2013 (http://www.afi-global.org/sites/default/files/pdfimages/AFI_MFSWG_guidelinenote_TechRisks.pdf)
- Fraud in Mobile Financial Services, Mudiri, MicroSave, 2012 (http://www.microsave.net/resource/fraud_in_mobile_financial_services#.VmWI9E10xes)
- Risk Management in Mobile Money, Lake, IFC, 2013 (http://
- www.ifc.org/wps/wcm/connect/37a0868042366698d8220ae0dc33b630b/Tool+7.1.+Risk+Management.pdf?MOD=AJPERES)

In addition, a comprehensive list of potential risks is included in the Risk Database section of this publication and can be used for reference.

Step 2: Historical review

The risk identification process will begin with a retrospective view on risk, taking into consideration risks that have been tolerated, treated, or realized throughout other project life cycles, including past product and channel implementations from your own institution or others within the market. The historical review will be done through secondary research of internal risk management documentation, as well as external sources such as industry contacts and the media.

Step 3: Current assessments

The current assessment of the DFS development takes a critical look at the current state of the implementation to understand what risks are most likely to exist. The implementation assessment will include an analysis of the current financial model, product specifications, business model, technology development, regulatory approvals, competitor analysis and market research. Using the risk categories described above, the risk team can start to put together the long list of potential risks. Many risks will start to emerge as the team explores the product definitions, the agent and distribution strategy, agent contracts, technology partner contracts, the local regulatory guidelines, the technology specifications, the operating procedures manuals, the financial projections, market research, or other documents that are available for review. Keeping in mind the risk categories, the team can also be asked to identify all possible risks that they recognize as relevant for their areas of operations. At this stage, it is important to list as many risks as possible, without judging their importance.

Step 4: Brainstorming

To complement the historical and current assessments, creativity techniques can be used for brainstorming sessions that may include external experts or facilitators.

Step 5: Record all risks identified in a risk register

This is the first step in the development of a risk register. All identified risks should be recorded including name, description, and owner, as well as any notes on preliminary responses to the risk that arise during the identification phase. At this stage, the list is meant to be as exhaustive as possible. During the evaluation stage, risks will be ranked and categorized in order to decide on relative importance.

Table 4: Example of the Risk Identification Stage for DFS Strategic Risk

Risk Type: Strategic Risk				
Name	***Description***	***Cause***	***Effect***	***Owner***
The DFS fails to reach sustainability in the timeframe designated	The DFS does not meet revenue and expense targets in specified timeframe	Poor product offering, poor channel management, poor management of resources, poor forecasting	Results in negative net revenue and return on investment.	Head of Agent Banking/ Mobile Money
Provider does not fully understand its target market for DFS.	An incorrect understanding of the customer needs and available resources	Poor strategy development, poor market research, poor consumer testing of the product or channel	Leads to development of inappropriate products and poor uptake and usage	Head of Marketing
Provider does not fully invest in resources required to meet targets.	Staffing for sales support is under-resourced	Long term investment needs of DFS channel is not understood or appreciated by management and board.	Provider is unable to meet targets for agent acquisition, and thus revenue targets are not achieved and sustainability is not reached.	Head of Sales
Competition	Competitors are gaining market share	Competitors providing superior service or lower prices.	Customers migrate to other providers	Head of Agent Banking/ Mobile Money

Section 3: Analyze and Evaluate

Once all risks have been identified, the process of analysis can take place in order to evaluate and prioritize them. Qualitative methods for analysis are the most commonly used, such as developing a scoring and ranking system, as described below:

Qualitative

Qualitative analysis allows you to start ranking the importance of the risks identified, and begins with the evaluation of characteristics and priorities based on pre-qualified metrics defined during the risk planning process. The qualitative analysis builds on the risk identification process to define risk and evaluate causes and impacts. Risks may be categorized based on source or cause, or by impact, in order to facilitate the development of risk responses during the qualitative analysis. The final output of a qualitative analysis will be the definition of the risk, the probability, and the potential impact. For example, the risk of competitors gaining market share is given a probability of 3 based on the fictitious example of a financial institution in highly competitive environment with low barriers to entry, and a potential impact of 3 based on some losses in financial revenue, but not complete losses as customer loyalty is high for this particular institution.

The steps to qualitative analysis are described below:

Step 1: Assign probability and impact

For each risk identified, a probability and impact qualitative assessment should be performed. Impact is the potential loss if the risk is realized. This could be financial loss, reputational loss, or legal or regulatory penalties. Impact can be measured on a scale of 1-5, 1 being the lowest and 5 being the highest. A measurement of 1 represents a negligible impact, 2 is low, 3 is moderate, 4 is high and 5 is extreme.

Probability is the assumed likelihood that the event will occur. It is also assigned on a scale of 1 – 5, with 1 being a remote possibility, 2 is unlikely, 3 is possible, 4 is likely and 5 is an almost certainty that the event will occur. A risk rating is then quantified by multiplying the ranking assigned to both probability and impact to produce a combined score for a particular risk.

Step 2: Risk analysis

The risk analysis is written documentation for the risk register that includes an analysis of the causes and effects of the risk; description of why the probability and impact were assigned as such; any secondary risks; priority; timeframe of when they might occur; and potential ways to treat.

Risk Prioritization

Step 3: Rank risks based on qualitative and quantitative risks

Risks can now be prioritized based on potential impact and probability. Using the qualitative ranking methodology, risks with the highest combined probability and impact score will be ranked highest, and those with the lowest combined score will be ranked lowest. If using the quantitative methodology, those with the highest R-value would be ranked as the highest risk. Ranking of the risks by priority will allow the project team to work towards risk strategies for each risk by working on the most important ones first.

Step 4: Decide which risks are worthy of treatment responses

Using the quantitative scoring, the institution can now decide whether to tolerate, treat, transfer or terminate the risk. Scoring thresholds may be used such as: 1 – 5: Accept Risk, 6 – 12: Control Risk and 13 – 25: Transfer or Avoid.

Figure 8 Qualitative risk ranking matrix

	Impact				
Probability	Negligible (1)	Low (2)	Moderate (3)	High (4)	Extreme (5)
Certain (5)	5	10	15	20	25
Likely (4)	4	8	12	16	20
Possible (3)	2	6	9	12	15
Unlikely (2)	2	4	6	8	10
Remote (1)	1	2	3	4	5

Once the analysis is complete, the risks should be categorized by type or priority, and recorded in the risk register.

Table 5: Example of the Risk Evaluation Stage for DFS Strategic Risk

Name	Description	Cause	Effect	Owner	Probability (1 – 5)	Impact (1 – 5)	Combined Score	Ranking
The DFS fails to reach sustainability in the timeframe designated	The DFS does not meet revenue and expense targets in specified timeframe	Poor product offering, poor channel management, poor management of resources, poor forecasting	Results in negative net revenue and return on investment.	Head of Agent Banking/ Mobile Money	2	3	6	#2
Provider does not fully understand its target market for DFS.	An inadequate understanding of the customer needs and available resources	Poor strategy development, poor market research, consumer testing of the product or channel	Leads to development of inappropriate products and poor uptake and usage	Head of Marketing	1	2	2	#4
Provider does not fully invest in resources required to meet targets.	Staffing for sales support is under-resourced	Long term investment of DFS channel is not understood or appreciated by management and board.	Provider is unable to meet targets for customer acquisition and activation, and thus revenue targets are not achieved and sustainability is not reached.	Head of Sales	1	3	3	#3
Competition	Competitors are gaining market share	Competitors providing superior service or lower prices.	Customers migrate to other providers	Head of Agent Banking/ Mobile Money	3	3	9	#1

Section 4: Risk Strategies

At this stage in the process, all risks should have been assessed and ranked based on probability and impact. Based on the risk acceptance thresholds set out in the planning process, the project team will now be able to identify which risks will be tolerated, treated, transferred, or terminated. Risks with low probability and low impact are most likely to be tolerated and no further action is required. For those risks that require treatment, transfer, or termination, a strategy must be developed.

Step 1: Develop risk termination strategy

Risk termination is done at the highest levels of combined probability and impact. It involves taking actions required to ensure that either the threat cannot occur or it can have no significant effect on the project. The spectrum of risk termination strategies includes a complete cancellation of the DFS implementation, or changing the fundamentals of the business strategy, to redefining product specifications or agent management strategies.

Step 2: Develop risk transfer strategy

Risk transfer strategies are applied when the risk can be transferred to a third party that is better positioned to address a particular threat. Agreements are required with a third party that clearly defines which party covers the other party's liabilities. An example of a risk transfer strategy relates to robbery of the agent's cash at the agent's premises. This risk can be transferred through the purchase of theft insurance either on behalf of the agent, or as a requirement for agents to purchase insurance for themselves as part of the agent agreement.

Step 3: Develop risk treatment strategy

Developing the risk treatment strategy will be one of the largest tasks undertaken by the risk management project team. Deciding on treatment strategies may require a compromise, since some proposed responses may be mutually exclusive or counterproductive. For example, mitigating the risk of excessive time delays to launch a service could cost money, thereby creating new risks by increasing pressure on the budget. Risk treatment strategy development also needs to take a holistic view of all proposed responses and make sure these are coherent.

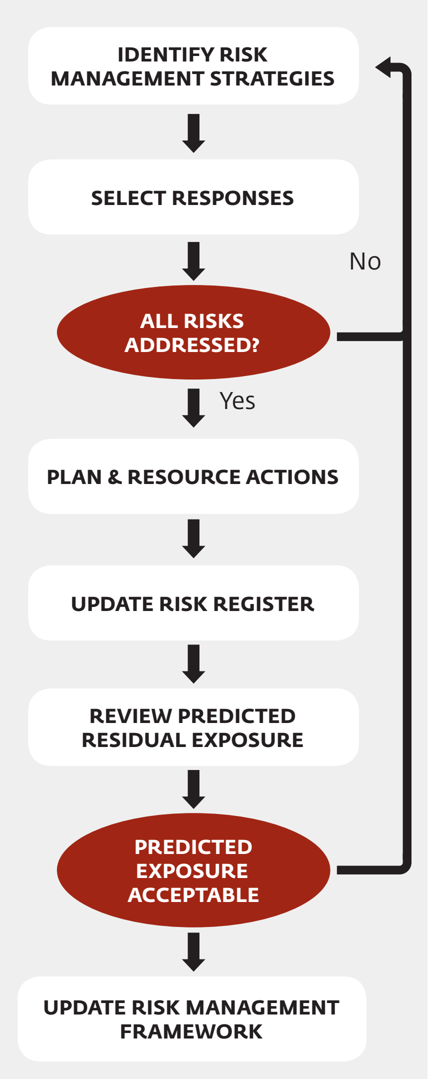
Risk treatment may include policies or actions that will reduce the likelihood or impact of the specific risk, thus reducing its score to an acceptable range before the project begins, or an incremental application of the treatment strategy that is implemented as risk becomes greater. Risk treatment strategies may also include response strategies on how to control damage only if and when risk is realized.

In general, treatment strategies should be appropriate, timely, cost-effective, feasible, achievable, agreed-upon, assigned, and accepted. At this stage in the process it is important to involve any relevant operations resource to ensure that the risk is being tackled from a practical "bottom-up" approach to prevent the creation of inappropriate or unworkable strategies. Any proposed risk treatment strategy should meet the following criteria:

- Consistent with organizational values, the objectives of the DFS business plan, and management expectations;
- Technically feasible;
- The project team or risk owners should have the ability and resources to carry out action required;
- Achieve balance between reduction of the risk impact and the ability to meet project objectives.

Risk treatment strategies are required to cover all risks exposed. Multiple strategies can be used to ensure there is no residual exposure as per Figure 6 below.

Figure 9: Steps involved in developing risk mitigation strategies


IDENTIFY RISK MANAGEMENT STRATEGIES
SELECT RESPONSES
No
ALL RISKS ADDRESSED?
Yes
PLAN & RESOURCE ACTIONS
UPDATE RISK REGISTER
REVIEW PREDICTED RESIDUAL EXPOSURE
PREDICTED EXPOSURE ACCEPTABLE
UPDATE RISK MANAGEMENT FRAMEWORK

Source: Project Management Institute: Practice Standard for Project Risk Management

Step 4: Develop risk treatment tactical response

Once the risk treatment strategies have been developed, a tactical, action-oriented response also needs to be developed for each strategy. The tactical responses should be integrated into DFS documentation such as the business plan or work plans.

Step 5: Develop Key Risk Indicator

Detection of event occurrence can be conducted through monitoring of Key Risk Indicators associated with each identified risk. The Risk Database section found in the Tools Chapter of this handbook has examples of appropriate KRIs to be used to measure and detect event occurrence. Acceptable KRI parameters should be developed and agreed on by management and the risk committee to allow project managers to proceed with escalation procedures if and when flags are triggered by non-performance of KRIs. Parameters and limits should be established by the risk function or board risk committee. They are generally a reflection of the risk tolerance of the institution.

Step 6: Record risk strategies in register

Lastly, the risk strategies are to be recorded in the register along with the previously documented information for each risk identified.

Table 6: Example of the Risk Strategy Development Stage for DFS Strategic Risk

Using the scoring thresholds of:

Risk Level	1 – 5	6 - 12	13 - 25
Action	Tolerate	Treat	Transfer or Terminate

For the risk identified in Table 5, risks ranked 3 and 4 can be tolerated as they have a combined score of less than 5. Risks 1 and 2 will require a treatment strategy because they fall in the control threshold of scores between 6 and 12.

Strategic Risk #1:

Risk Category:	Strategic Risk
Secondary Category:	Financial Risk
Name:	Competition
Description:	Competitors are gaining market share
Owner:	Head of Marketing
Cause:	Competitors providing superior service or lower prices
Effect:	Customers migrate to other providers
Probability:	3 out of 5
Impact:	3 out of 5
Risk Strategy:	Treat
Treatment Strategy:	• Perform research to understand competitor offering, its strengths and weaknesses • Monitor call center logs for complaints about service levels • Promotions to keep customers engaged and active • Cross-sell other products and services to create customer stickiness
Treatment Tactical Response:	• Re-evaluate product and channel design, pricing, and commission structures • Conduct market research to further understand market demand and develop renewed value proposition
Key Risk Indicator:	% Market Share

Strategic Risk #2:

Risk Category:	Strategic Risk
Secondary Category:	Reputational / Financial Risk
Name:	The DFS fails to reach sustainability in the timeframe designated
Description:	The DFS does not meet revenue and expense targets, which results in negative net revenue and return on investment
Owner:	Head of DFS
Cause:	Poor product or channel design, misunderstanding of market demand and/or competition
Effect:	Loss of investment
Probability:	2 out of 5
Impact:	3 out of 5
Risk Strategy:	Treat
Treatment Strategy:	• Use market research and industry benchmarks to base assumptions • Ensure targets are realistic and aligned with KPIs • Ensure that sufficient resources (people/ funds) assigned to achieve targets • Monitor performance and update strategy as needed
Treatment Tactical Response:	• Iterate financial model as implementation progresses • Re-evaluate pricing and commission structures • Conduct market research to understand market demand • Perform promotional activity to stimulate uptake
Key Risk Indicator:	• Net revenue • Active customers • Transactions per customer • Active agents • Customers per agent • Float interest rate

Section 5: Monitor and Review

The effectiveness of the risk management framework depends on how well it is implemented. Implementation includes initiating work on the tactical responses addressed in Section 4, as well as periodic review and reassessment. As the DFS matures and evolves, new risks will appear, and the probability and impact of previously identified risks will change over time.

The risk management framework and the risk register are living documents. The project team will decide on reporting and reassessment intervals at the onset of the risk management framework development. It is recommended that risk reporting is conducted quarterly and full reassessment is conducted annually.

Step 1: Risk Reassessment

In addition to regular review, it may be necessary to conduct a reassessment if one of the following occurs:

- Occurrence of a major or unexpected event;
- A fundamental change to the business plan or DFS management strategy;
- A new type of service is offered via the DFS;
- End of implementation phase.

Step 2: Track risks for period

For each period reported on, each risk will be reported as either:

- Did not occur
- Occurred and contingency plan invoked
- Occurred and impacted project (time, cost, and quality)

In addition to reporting on the existing risk register, it should also be reported if any new or previously unidentified risks have been noted, the effectiveness of the risk strategies, or any changes to cause and effect of risks within the register. It is also very useful to track the risk profile for key risks over time, as changing circumstances (including the implementation of risk prevention and mitigation strategies) can make the risk of a specific event occurring more or less likely, or change its potential impact.

Summary

In order to successfully implement a DFS strategy, a standardized structure for building a risk management framework is required to support and sustain the operations. The process begins with establishing the context, including building the team and getting full buy-in from management and the board. The most important part of the framework development is the risk identification, evaluation, and treatment strategy development. A broad group of individuals with diverse backgrounds should participate in the risk identification process. Desk reviews, historical reviews, and reviews of current project aspects can all be used to tease out all the possible risks associated with the DFS implementation. Once identified, appropriate and consistent assessment methodologies can be used to assess and rank the priority of the risk identified. Development of treatment strategies includes deciding whether to tolerate, treat, transfer or terminate the risk, and to develop the appropriate strategy to do so. Once completed, the risk management framework can be monitored and reviewed. It is very important that the risk framework is a living document, and used to actively report on risk occurrence, as well as to be reviewed and updated periodically or upon occurrence of a major event.

04_

Part IV

Insights and Tools

Lessons Learned

Most institutions interviewed in our research had some type of risk management framework for their core business that had been extended to DFS. The implications of how DFS change the risk profile, reducing some risks but adding new potential liabilities, are understood by some whilst others are unsure of how to react. There is a growing need for guidance about DFS risk management that is relevant and accessible to all types of providers. Key lessons extracted from our research and discussions with a range of providers are summarized in the following observations. Most importantly, there is a need for comprehensive risk management frameworks.

As DFS around the globe continue to grow and extend the range of services available, they become more vulnerable to unforeseen or new risks. Increased public awareness of services and increased volume and value of transactions may attract attention from unwanted places and people. To protect these new and growing businesses, their customers, and their partners (such as agents), there is a clear need for most DFS providers to improve risk management awareness, approach and implementation. Whilst a minority has developed effective risk treatment strategies, many DFS providers currently have a superficial approach, with little to no risk treatment in place.

Risk registers have been created by some DFS providers, but it is not clear that these are widely used in the running of the business. There generally seems to be limited understanding and awareness[14] of how to implement them. The registers are typically limited to risks that would result in immediate financial losses, such as fraud or technical issues, and do not cover broader and more deeply rooted risks such as strategic risks, reputational risks, cyber risks, partnership risks, or political risks. Their creation is often seen as the end goal (to appease auditors or governance committees) rather than the start of an ongoing process to reduce the risks to the organizations. Finally, they are not often clearly or critically linked to the achievement of objectives.

[14] In preparation for this publication, the IFC interviewed a range of DFS providers, technology providers, NGOs, and other related organizations

LESSON 1

Technology, strategic, and agent management risks can all lead to reputational risk

If customers cannot access their money when they need it, there is a potential reputational risk that can lead to reduced customer uptake, decreased activity rates, and dormant accounts: all of which will inflict potentially large losses on a provider as it cannot meet targets set out in its business plan. When that happens, there are even more serious repercussions if boards and management lose confidence and reduce budgets or reorient business resources and rely on alternative (non-DFS) strategies to drive customer and revenue growth. Thus, it is of utmost importance that the customer experience is seamless, with superior customer service and competitive pricing. Technology, strategic, and agent management risk all play a role in providing a superior customer service and include:

- Products meet the needs of the customers
- Channel design meets the needs of the customers
- Pricing is competitive
- Accounts can be open at the agents and ideally accessed by the customer instantly
- Customers can also access their accounts through other channels if required, such as branches and ATMs
- Well-staffed, well-trained call centers
- Multiple customer service points including call centers, as well as email, SMS, roaming sales staff and trained branch staff
- Technology that is always working, i.e. data and voice connectivity is available; software service is available; hardware device is operable; and there are no transaction delays or failures during any point in the communication
- Accurate and timely SMS receipts
- Customers are always refunded for fraudulent activity
- Fees are easy to understand
- Menus are easy to follow
- Agents are always available and liquid
- Agents are well trained to service customers
- Agents are clearly and consistently branded

LESSON 2

Fraud can have a huge impact on reputation

Fraud can cause direct financial losses as a result of unauthorized withdrawal of funds or unauthorized creation of e-money. Moreover, the full impact of fraud can extend further. When made public, fraudulent activity is known to reduce consumer confidence in DFS, as well as core services of the provider such as MNO voice or retail banking businesses. Consumer confidence issues can also spill over to other providers, and affect the market as a whole. For this reason, there have been several major fraud incidents with associated losses which the providers have prevented from becoming public. Others have not kept their losses secret, to the detriment of both their DFS and core business. One institution implemented a mitigation strategy of going to the press first about a case of fraud in the hope that it would minimize the reputational damage, but it was felt that in hindsight this just brought attention to the issue and scared customers. There is still disagreement among providers about the best way to handle large cases of fraud. Because of the potential damage fraud can inflict on the whole DFS market, there is a good case for better industry sharing of experiences and lessons learned. However the challenge of persuading providers, who are also competitors in DFS and other areas, to cooperate should not be underestimated.

LESSON 3

The utility of the call center

The utility of the call center is wide-reaching, well beyond the primary goal of resolving the needs of customers. Call centers can be used for customer education, customer feedback, and improving the brand value of the institution. Call center operating hours should be extended to evenings and weekends to service high call volume when customers are most likely to be transacting and cannot go to a branch or service center. There should be a process to alert and update call center staff to any system issues so that they can reassure concerned callers. Call centers can also be used for risk management purposes by utilizing call center logs to identify potential risks to the DFS, as well as to monitor key risk indicators.

Once issues are raised to a call center, institutions should aim to resolve the majority of them within the first call. Anything longer, or requirements for follow up calls, will reduce trust in the service and have reputational risks and potential financial losses.

LESSON 4

Poor reconciliation and settlement processes leave institutions open to potential losses

Settlement and reconciliation is a laborious process that can have significant impacts on operational costs as well as reduce customer confidence if transactions end up in suspense accounts for significant periods of time. For example, refunds of debit without disbursement transactions can take up to one week, leaving customers frustrated and cash-poor. Automatic, daily reconciliation is recommended not only to reduce the numbers of suspense transactions, but also as a useful tool in early fraud detection.

LESSON 5

Choose partners carefully, and then hold them accountable

Partners can refer to other providers that collaborate on joint products or services, or vendors that provide technology or agent management services for example. In the context of joint products, there is a strong strategic risk if there is a high reliance on a single partner; the partner may not have exclusivity agreements, and may be using the partnership to learn and replicate on their own.

All partnerships should be entered only after thorough due diligence and comprehensive discussions on roles and responsibilities. Partnership agreements can be in the form of contracts, memoranda of understanding between providers, or service level agreements with vendors. MOUs and SLAs should clearly define the outputs of each side, fault escalation paths, service availability, costs, payment terms, intellectual property rights, and confidentiality agreements. For the smaller partner the most critical element of such partnerships is protection and clarity in the partnership agreement as to when and how the partners can enter into competition with each other. Well thought out agreements can go a long way in protecting an institution from unanticipated failure to deliver or lack of compliance from partners. However, it is worth noting that agreements cannot always guarantee accountability. If the partner is very big and more powerful, you may not be able to hold it accountable, or if the partner is very small, it may simply not have the capacity to meet the requirements set out in the agreements. In most instances, it is wise to avoid exclusivity. For technical service delivery, multiple channel suppliers should be sought wherever possible.

Conclusions

This handbook provides a guide to the kind of risks that may be encountered in the deployment of a DFS strategy. Many of the case studies point to the overarching importance of strategic risk, the risk that the strategy fails to meet its objectives due to deployment of inappropriate services, poor technology, customer behavior not aligning with initial models, or unanticipated market developments. It is always risky to provide a list of risks, and possibly more so to provide a list of future risks, but a number of trends are already emerging that will probably shape the evolution of risk management in DFS.

- One of the most important risks is linked to the speed of innovation and disruptive change to existing DFS channel strategies which can make a DFS strategy redundant before the technology is fully deployed. The rate of change in technology and platforms is unprecedented. Not only do service providers need to determine what platforms to support, but customer requirements change fast. A bank in Mozambique deployed POS devices in taxis; two years later, Uber was serving the same market in seven of Africa's largest cities with smartphones and direct billing to credit cards.
- With the rapid increase in smartphone usage, more and more DFS deployments will rely on either the customer's or the agent/merchant's smartphone. This should reduce some of the difficulties operators have experienced with managing POS technology and with the limitations of SMS and USSD. Financial institutions wishing to develop a DFS strategy will need to develop the technical knowledge on how to manage such risks.
- In markets such as Kenya where agency banking has been successful, merchants now have a bewildering number of POS devices and phones on which to handle transactions for an increasing number of institutions. It is thus probable that agent banking will evolve from a service in which each bank seeks to enable as many agents as possible to a situation in which any merchant can handle a deposit or withdrawal on a single device for any bank or MNO provided they have signed up to a standard set of rules. This will once again change the competitive dynamics. Some institutions will specialize in agent services, while others will focus on customer services and use the agent banking services provided by others.

- Regulation of DFS enabled services such as mobile money and agent banking is likely to increase and will also change the competitive dynamics. In an increasing number of jurisdictions, regulators are starting to mandate interoperability between payment services including mobile money, as well as preventing providers from signing exclusive arrangements with agents.
- Although cash remains popular in all markets in the world, as electronic transaction costs fall there will be a gradual reduction in the need for cash in/cash out services, which need to be factored into the DFS strategy. In the long term, as reliance on cash declines, some merchants will see their cash sales decline and will thus be less able to support the cash liquidity requirements of agent banking services.

No DFS provider will be able to escape the risks associated with the implementation of new technology and business models. The case studies have highlighted however how it is possible to manage these new risks in order to achieve business objectives in support of the growth of financial inclusion.

Tools

Risk Management Checklist

Risk architecture

- Statement produced that sets out risk responsibilities and lists the risk-based matters reserved for the board
- Risk management responsibilities
- Arrangements are in place to ensure the availability of appropriate competent advice on risks and controls
- Risk aware culture exists within the organisation and actions are in hand to enhance the level of risk maturity
- Sources of risk assurance for the Board have been identified and validated

Risk strategy

- Risk management policy produced that describes risk appetite, risk culture and philosophy
- Key dependencies for success identified, together with the matters that should be avoided
- Business objectives validated and the assumptions underpinning those objectives tested
- Significant risks faced by the organisation identified, together with the critical controls required
- Risk management action plan established that includes the use of key risk indicators, as appropriate
- Necessary resources identified and provided to support the risk management activities

Risk protocols

- Appropriate risk management framework identified and adopted, with modifications as appropriate
- Suitable and sufficient risk assessments completed and the results recorded in an appropriate manner
- Procedures to include risk as part of business decision-making established and implemented
- Details of required risk responses recorded, together with arrangements to track risk improvement recommendations
- Incident reporting procedures established to facilitate identification of risk trends, together with risk escalation procedures
- Business continuity plans and disaster recovery plans established and regularly tested
- Arrangement in place to audit the efficiency and effectiveness of the controls in place for significant risks
- Arrangements in place for mandatory reporting on risk, including reports on at least the following:
  - » Risk appetite, tolerance and constraints
  - » Risk architecture and risk escalation procedures
  - » Risk aware culture currently in place
  - » Risk assessment arrangements and protocols
  - » Significant risks and key risk indicators
  - » Critical controls and control weaknesses
  - » Sources of assurance available to the Board

Source: Enterprise Risk Management (ERM) and the requirements of ISO 31000, AIRMIC, Alarm, IRM: 2010

Risk Register Template

Risk Category:	Choose one of: Strategic, Regulatory, Operational, Technology, Financial, Political, Fraud, Agent Management, Reputational, Partnership
Secondary Categories:	Choose one or more of: Strategic, Regulatory, Operational, Technology, Financial, Political, Fraud, Agent Management, Reputational, Partnership
Name:	Name of risk
Description:	Short description of risk, which may need to include a brief cause and effect in order to accurately describe
Owner:	Person responsible for monitoring risk and deploying treatment strategies
Cause:	The reason why the event occurs
Effect:	The impact the risk has if realized
Probability:	The likelihood the risk will occur. Can be ranked on a scale of 1 - 5 or assigned a percentage of 0 – 100%
Impact:	The potential losses if the event was to occur. Can be ranked on a scale of 1 – 5 or assigned a value of the actual costs of risk realization
Risk Strategy:	Choose one of: Tolerate, Treat, Transfer or Terminate
Treatment Strategy:	Policy implication of the institution to control risk either before, during or after event occurrence
Treatment Tactical Response:	Specific actions to be taken in the case of event occurrence
Key Risk Indicator:	An indicator used for the early warning that the potential of a risk's adverse effects may occur
Current status:	Choose one of: Has not occurred, Occurred and treated, Occurred with impact

Risk Database

Risk[15]	Description	Type of Institution	Policy Options & Potential Mitigation Tools	Key Risk Indicators
Strategic Risk				
The DFS fails to reach sustainability in the timeframe designated.	The DFS does not meet revenue and expense targets and results in negative net revenue and return on investment.	Any	Use market research and industry benchmarks to base assumptions. Iterate financial model as implementation progresses. Ensure targets are disseminated and aligned with KPIs. Monitor performance and update strategy as needed.	Net revenue Active customers Transactions per customer Active agents Revenue generating transactions Float interest earned
Provider does not fully understand its target market for DFS.	An incorrect understanding of the customer leads to development of products and channels not suited for the target customer.	Any	Use market research to develop product specifications, channel design, and decide on appropriate technology interfaces. Monitor customer uptake and activation. Use focus group discussions, call center logs and agent feedback to inform DFS design. Lessons learned in other markets.	Active customers vs. registered customers Active agents vs registered agents Transactions per customer
Provider does not fully invest in resources required to meet targets.	Staffing and marketing are under-resourced and provider is unable to meet targets for customer acquisition and activation.	Any	Ensure adequate resources are allocated upfront for staffing and marketing based on industry benchmarks and local costs of staff and marketing activities. Commit resources throughout period until sustainability is achieved or strategy revised.	Staff costs actual and as a % of total costs Marketing costs actual and as a % of total costs.
De-prioritization of DFS products or channels	Poor performance leads to de-prioritization of DFS and organization reorients around competing priorities.	Any	Resolve the main issues within the DFS department (e.g. technological, reputational, or operational risks). Execute market research to identify customer needs vs the service being offered.	Net revenue Active customers Active agents
Competition	Competitors are gaining market share due to superior service or lower prices.	Any	Improve service quality through agents and call center. Re-evaluate pricing and commission structures. Re-evaluate product features.	Market share of active customers Market share of transactions

[15] Authors own as well as sourced from:
Mobile Financial Services Risk Matrix, USAID, 2010
Fraud in Mobile Financial Services, Mudiri, MicroSave
Mobile Financial Services Technology Risks, Alliance for Financial Inclusion (AFI), 2013
Risk Management in Mobile Money: Observed Risks and Proposed Mitigants for Mobile Money Operators, Lake, IFC, 2013
Digital Financial Services Risk Assessment for Microfinance Institutions: A Pocket Guide, The Digital Financial Services Working Group, 2014
Risk Management Case Studies, Fidelity Bank, Kopo Kopo, FINCA DRC and Tigo Tanzania, IFC & Genesis, 2015

Risk	Description	Type of Institution	Policy Options & Potential Mitigation Tools	Key Risk Indicators
Customer cannibalization	Branches and agents poaching each other's banking customers to meet their own KPIs.	Bank or MFI	Develop joint KPIs to prevent silo operations.	Customers served through agents vs branches Services offered through agents vs branches
Competitive threat from partner	Partner is directly competing with provider to acquire merchants, agents or customers resulting in slower growth rates or loss of customers.	Any	MOUs with partners to define exclusivity and ownership of customer. Provide quality service to customers and agents. Diversify dependence on partner by using multiple partners. Marketing and awareness campaigns. Market research for additional differentiators and product innovations. Develop joint marketing strategies.	Market share of active customers Market share of transactions
Lack of network interoperability prevents customer from transaction with desired party.	Closed loop networks with no capability to transfer funds between account holders of different account providers' payment networks due to lack of interoperability.	Any	Integrate to other providers and allow customers to move funds between parties and perform off-net transactions.	P2P transaction volume Overall transaction volumes
Interoperability increases churn.	Developing interoperable systems with partners may lead to loss of core business customers as they no longer need to be your customer to access your services.	Any, but mainly MNOs	Monitor transactions during pilot phase for trends in cash movement and customer behavior. Joint marketing campaigns. Incentives to drive customer retention.	Market share of active customers Market share of transactions Customer activity
Key person risk	Management, founders, or board members leave organization which has direct impact on sustainability or leads to de-prioritization of the DFS.	Any	Deploy team approach to projects. For each position, have a substitute in waiting. Ensure sharing of learning and information.	Net revenue Total budgets vs project expenses.
Financial Risk				
Provider loses customer funds due to failure of trustee bank.	The trustee bank becomes insolvent, trust accounts that are not legally segregated from the general pool of bank assets available to satisfy creditors may be pulled into the bankruptcy process, with access blocked.	MNO	Identify trustee bank through adequate due diligence to ascertain its financial stability. Trust funds holding the value of items in transit are legally segregated from the trustee's own assets in bankruptcy. Trust accounts are divisible and transferable. Diversification of deposits into multiple banks.	Capital adequacy of trustee bank ROE & ROA of trustee bank
Asset – liability matching	DFS customers may be more likely to deposit small, short term deposits compared to other bank customers, meaning that the provider is less able to intermediate funds into longer term, more profitable revenue sources.	Banks, MFIs	Diversify the service to add savings capabilities as well as short term lending. Incentivize long term deposits through interest bearing accounts.	Average account balance Number of cash in and cash out transactions per month per customer

Risk	Description	Type of Institution	Policy Options & Potential Mitigation Tools	Key Risk Indicators
Credit risk of customers	On account of the new distribution structure, the clients may feel a diminished obligation to repay loans as they no longer have a direct relationship with the provider.	Banks, MFIs	Closely monitor customer behavior patterns. Develop systems to alert loan officers when loans are not repaid on time. Incentivize agents to collect loan repayments similar to incentive structures for loan officers.	Portfolio at Risk
Credit risk of agents and merchants	Non-repayment of loans given to agents or merchants.	Any	Develop credit risk policies, loan due diligence procedures, and diversify credit risk. Implement loan loss provisions based on portfolio aging. Use algorithms for validating loan approvals and monitoring ongoing loan performance.	Portfolio at Risk
Foreign Exchange Risk	Local currency devaluation increase costs and devalues assets.	Any	Hedge borrowings in foreign currency.	FX rates
Settlement risk	The risk that one party fails to deliver funds to another party at the time of settlement.	Any	Use real time gross settlement systems for bank transfers. For MNOs, bilateral agreements to control for settlement.	Number of transactions in suspense accounts Time it takes to reconcile and settle transactions in suspense accounts
Technology Risk				
Breach of customer or agent account	Customer or agent account is breached and access is gained to security credentials, account information, or transaction history, which could result in loss of funds, processing illicit transactions, or identify theft. Customer account information could be improperly accessed through: SMS history Poor encryption of WAP Cross-site scripting of USSD sessions Unauthorized access or usage by provider staff or agents	Any	Institute controls to reduce the likelihood for unauthorized release, or theft, of personal information through encryption, two -factor authentication, and tiered user rights.	Algorithms for detecting suspicious behavior Call center escalation logs

Risk	Description	Type of Institution	Policy Options & Potential Mitigation Tools	Key Risk Indicators
Customer cannot access account due to lack of system availability and/or transaction failure.	Customer cannot access account through application or agent due to: Mobile network is not available The provider's system is experiencing temporary system downtime.	Any	The provider should test end-to-end transaction availability on a periodic basis. All transaction interfaces to be defined with clear completion boundaries, allowing clear rollback procedures in the event of uncertainty. Service level agreements with system providers and partners and penalties for non-conformance Agreed escalation processes to resolve issues. System upgrades. Use USSD as a fallback to 3G-enabled POS to reduce reliance on data connectivity.	End-to-end transaction success rate
Malware	Viruses, Trojans, or worms infect files, gain remote access, install malicious software to steal data, conduct unauthorized transactions, or block authorized usage.	Any	Use a combination of anti-virus software, fire walls, intrusion detection systems, proxy servers, web content, email attachment filters, and data encryption techniques. Develop procedures for staff, agents and customers to report suspicious activity.	Reported successful attacks on the service
Transaction replay by the network	MNOs often have automatic retry requests to deliver an SMS to a destination if it is not successful on the first try. When used in mobile money transactions, some systems can interpret as multiple transaction requests.	Any using SMS applications	Disable retry requests. Use SMS receipts for transactions for customers to monitor if there are duplicates.	System reports on duplicate transactions
Transaction delays	System lags may cause transaction delays or receiving of SMS receipts to be delayed.	Any	Limit system's ability to retry transactions. Educate agents and customers to do balance checks if they do not receive SMS receipt immediately.	Complaints of duplicate transactions Calls to customer care about SMS not received
Hardware failure	POS devices fail due to poor construction or inability to connect to software.	Bank, MFI, or PSP	Service level agreement with hardware providers including penalties for non-conformance. Maintenance agreement with hardware provider.	Transaction failure rate POS failure rate
Loss of data	Breakdown of primary storage and backup facility (including cloud-based systems) resulting in loss of transaction records.	Any	Provide separate mirrored databases to record all transactions in real time. Export transaction information to storage regularly.	Transaction records lost
Hosting environment failure	System is not available because of technical issues with the DFS hosting environment.	Any	Regular technical & financial audit of hosting environment and vendor. Use of service level agreements with hosting organization/ storage vendor. Use of cloud-watch software to monitor health of cloud provider. Documented procedures for service failure and disaster recovery.	System availability Number of outages Time taken to recover from outages

Risk	Description	Type of Institution	Policy Options & Potential Mitigation Tools	Key Risk Indicators
Regulatory Risk				
Potential customers do not have ID or other KYC requirements	When initially registering for an account, the customer is unable provide ID.	Any	Customer education campaigns to acquire ID and KYC requirements before account registration. Regulatory lobbying to allow for reduced requirements and/or ID substitutes	Customer awareness vs. customer registration Agent feedback on customers refused registration
Transaction taxes	Governments decide to tax transaction fees in order to increase revenue which could negatively impact customer demand.	Any	Lobby government and opinion formers to prevent taxation Potentially lower fees (i.e. pay all or part of the tax on behalf of customers)	Sharp or unexplained reduction in transactions
Agent does not adequately KYC customer	Agents may not fully comply with KYC requirements as commissions are designed to incentivize account opening and performing transactions.	Any	Agent education. Align incentives to properly registered customers only. Where regulations allow, open tier one accounts with reduced KYC until full information can be collected. Mystery shopping. Penalties for non-compliance.	Percentage of customer registrations rejected by DFS provider
Changes in regulations	Regulator changes laws that are no longer conducive for DFS operations or prevent providers from obtaining licenses.	Any	Build alignment and communication channels with regulators.	Formal communication of impending regulatory changes Complaints from regulator of non-compliance
Lack of compliance	Provider does not comply with applicable laws and regulations resulting in fines, regulatory intervention and ultimately loss of license.	Any	Compliance department ensures full compliance with regulatory laws. Monitor any plans to change applicable regulations and provide feedback to regulator. Ensure the system is upgraded to comply with any planned changes to regulation.	Internal audit reports, external audit management letter Regulator compliance
Political Risk				
Inability to access accounts or conduct transactions.	Post-election violence, civil unrest, war, or terrorist activity disrupt normal business operations.	Any	Service disruption plan developed for agents and staff. Business Continuity plans. Communication plan.	Report number of hours or days without service Compare downtime with key competitors
Agent Risk				
Lack of agent availability	Customers cannot access funds or conduct transactions due to a lack of agents in their vicinity or existing agents are inaccessible due to excessive queues.	Any	Conduct agent recruitment campaigns in the vicinity of overburdened active agents. Ensure agent density coverage is adequate.	Number of customers per agent. Agent activity Customer activity rates

Risk	Description	Type of Institution	Policy Options & Potential Mitigation Tools	Key Risk Indicators
Lack of agent liquidity	Customer cannot perform cash out or cash in transaction because the agent does not have sufficient cash on hand or e-money.	Any	Use of agents and super-agents for liquidity. Use call center logs to identify problem agents and work with them to resolve liquidity issues. Roll out agents in conjunction with customer registration to ensure adequate incentives to manage customer needs. Reports to identify agents that are not meeting liquidity requirements. Manual/automated alerts to agents when their e-money float is running low. Pre-fund agent capital requirements through loans or lending institution partnerships. Mystery shopping and good agent management.	Monitor agent e-money balances Number of customer complaints about cash liquidity
Agent robbery	Agent is robbed.	Any	Require/recommend that agents purchase theft insurance. Educate agents not to keep excessive amounts of cash on the premises. Carry out background checks of potential agent employees, or suggest that agents do so. Agents to conduct daily reconciliations of transactions, float, and account balances. Require agent proximity to police. Physical cash security through safes, secured booths, etc.	Track and document agent robbery by area, time of day, nature of theft
Agent inactivity	Provider fails to properly identify, train and manage agents well and/or there are insufficient customers to keep agents active.	Any	Roll out agents in conjuncture with customer sign up. Monitor agent activity rates and increase education and monitoring for poor performing agents. Systems to flag and report early detection of inactive agents. Cease business with consistently inactive agents. Review incentive and pricing structures to ensure appropriateness.	Agent activity rate
Agent error	Data capture errors, key stroke errors, typos etc. made by the agent or staff that result in inaccurate registrations or transactions.	Any	Provide phone number look up to verify account name during transaction processing. Potentially require entry of key data twice to confirm. Agent training for owner/operator and agent staff. Agent call center for reversals and inquiries. Back-office processing unit to verify KYC details.	Transaction reversals rate Account registration rejection

Risk	Description	Type of Institution	Policy Options & Potential Mitigation Tools	Key Risk Indicators
Agent solvency risk	The inability for an agent to honor his/her liabilities and results in insolvency and closure.	Any	Agent due diligence to select only reputable and stable agents. Process to remove DFS branding and hardware from failing agent premises.	Agent closure rate
Poor quality customer experience at agents	Agent staff who serve customers may not have been trained by the provider and have a poor understanding of the service.	Any	Regular re-training for agent and all staff. Agent call center for inquiries. Mystery shopping and good agent management.	Customer activity rate Customer complaints
Agent branding	Inconsistent agent branding due to removal by agent/other merchandisers or inability to place branding due to presence of other branding materials.	Any	Make sure there is a contractual arrangement with agents to have a minimum branding standard at all agent outlets. Sales support to check branding and availability of other materials during regular visits. Mystery shopping.	Records of non-compliance made by agent managers
Agent business case	Risk that agents may not have enough customers or commissions to sustain operations.	Any	Well-structured agent incentives. Strategic rollout of agents with adequate customers and territory. Agent commission for account sign up to drive customer penetration. Agent support through agent officers and call centers and training.	Agent activity rate
Fraud Risk				
Customer defrauded by outside party				
Stolen identity	Customer identity is stolen and used to open an account or conduct fraudulent transactions.	Any	Consider use of biometric devices to reduce fraud. Adoption of policies and procedures to enhance fraud detection. Utilize PINs and conduct customer education on PIN protection. Good policies on PIN resets to deter fraudulent activity. Rapid collection of original documentation from the agent or account opening staff. Ideally get electronic documentation that can be transmitted to the provider immediately. Vetting agents for character during the appointment process.	Records of non-compliance made by agent managers

Risk	Description	Type of Institution	Policy Options & Potential Mitigation Tools	Key Risk Indicators
Impersonation of provider or agent	An individual poses as a provider employee or agent and accepts deposits or gains unauthorized access to customer accounts to conduct fraudulent activities.	Any	Educate customers to receive SMS confirmation before they handover cash. Customer education campaigns to identify valid agents and keep PIN secret. Call centers for customer complaints. Clear customer escalation and feedback process to report fraud cases and trigger market sensitization of the fraud. Daily reconciliations of payments and receipts against internal systems. Clear and consistent agent branding.	Records of non-compliance made by agent managers
Phishing	Fraudsters pose as official representatives of agents or providers to gain access to agent or customers' PINs, account capabilities, transaction records, or account balances.	Any	Minimize information reported on transaction reports to only what is absolutely necessary. Request customers to report any threats and fraud occurrences to law enforcement authorities. Awareness campaigns to educate agents and customers on account security and keeping PIN etc. secret. Develop clear procedures and guidelines for identification, communication and management of fraud.	Records of non-compliance made by agent managers
SIM swaps	A customer's (or agent's) SIM card is swapped for a new one without authorization. The holder of the SIM card can then access the customer's account and transact without their knowledge.	Any using mobile devices	Document a clear SIM swap process which limits people/organizations that can carry out SIM swaps and establishing time limits between the time that the SIM swap is carried out and the time it is implemented. Keep track of swaps carried out through reports.	Records of non-compliance made by agent managers
Voucher fraud	Vouchers and transaction codes that are generated to enable payments to merchants for pre-defined goods or for cash out are stolen and used without authorization.	Any	Develop clear processes that define generation of vouchers, expiry periods and notifications on expiry. Vouchers should not be visible to anyone except the recipient and when misplaced, the recipient can notify the business and get fresh ones re-issued directly. Preferably, in the case of unregistered customers, they must be required to register before they access funds.	Customer complaints
Customer defrauded by agent				
Unauthorized fees	Agent may overcharge or charge an additional unauthorized cash fee to the consumer.	Any	Providers use clear contracts that fully disclose all fees to be charged, tailored for various customer situations, including different languages and illiteracy. Service charges clearly posted at each agent's location. Disclosures reasonably comprehendible to all customer groups.	Customer complaints

Risk	Description	Type of Institution	Policy Options & Potential Mitigation Tools	Key Risk Indicators
Agent receives cash from client but fails to perform the transaction.	Agent receives funds from a service user but misdirects funds to the agent's own benefit.	Any	Customer education campaigns to verify the transaction has occurred before leaving the agent premises. Utilize call centers for customer complaints. Policies and procedures for agent misuse of customer funds including penalties and closure of agent.	Customer complaints
Agent pays out cash that proves to be counterfeit.	Agent may use cash out payments to distribute counterfeit currency or may pay out counterfeit currency received from customers without realizing it is counterfeit.	Any	Require agents to use counterfeit detectors to ensure they don't erroneously collect counterfeit funds. Make tools available to customers at agent shops. Customer education campaigns. Policies and procedures for agent misuse of customer funds including penalties and closure of agent.	Customer complaints
Unauthorized access to customers' PIN	Agents accesses customer PIN and uses it to withdraw funds. Due to poor customer literacy, customer may share PIN with agents willingly.	Any	Develop a comprehensive due diligence process for the recruitment of agents to minimize recruitment of agents with poor reputation or those likely to commit fraud. Carry out periodic and planned consumer and market awareness on PIN security, discouraging PIN sharing. Ensure that relevant campaign documentation is also in all outlets. Customer education to change their PINs when they receive them and keep them confidential. Customer education on how to perform transactions securely.	Customer complaints
Split withdrawals	Agents force customers to split withdrawals in a number of smaller transactions in order to trigger higher customer fees and higher agent commission fees.	Any	Use data analytics tools to flag suspicious transactions. Develop a comprehensive due diligence process for the recruitment of agents to minimize recruitment of agents with poor reputation or those likely to commit fraud. Carry out mystery shopping activities and channel audits. Policies and procedures for agent misuse of customer funds including penalties and closure of agent.	Duplicate transactions Customer complaints
Customer defrauded by provider internal staff				
Employees link wrong mobile numbers to bank accounts	Collusion between employees and fraudsters to link fraudsters' mobile numbers to the customers' accounts facilitating withdrawal of funds from the customers' accounts.	Any	Maintain separate accounts for receipts and disbursements to limit the exposure of clients to fraud. For accounts linked to wallets, ensure that customers sign authorization for account linkage. Use SMS receipts to notify customers of linkages. Bank audit of linked accounts.	Customer complaints

Risk	Description	Type of Institution	Policy Options & Potential Mitigation Tools	Key Risk Indicators
Illegal reversal of customer payments / transfers	Employees collude with the paying party and illegally reverse customer payments.	Any	Use SMS receipts to notify customers of transactions. Ensure maker/checker procedures for all reversals. Create reports to monitor suspicious customer and staff behavior.	Suspicious activity reports Customer complaints
Illegal transfers from mobile accounts	Illegal transfers by employees from customer accounts to fake accounts or accounts of fraudsters.	Any	Use SMS receipts to notify customers of transactions. Ensure maker/checker procedures for all reversals. Create reports to monitor suspicious customer and staff behavior	Suspicious activity reports Customer complaints
Agent defrauded by customer				
Agent takes in cash that proves to be counterfeit.	Counterfeiter manufactures false notes, deposits to account at an agent and then withdrawal valid currency from another agent.	Any	Agents use counterfeit detection tools. Agent education. Agent call center. Mystery shopping and good agent management.	Agent complaints
Unauthorized access of agent's device.	Customers access agent's transaction tools to conduct fraudulent transactions.	Any	Require agents to keep a separate business handset and SIM card if mobiles are being used and practice good handset management practices. Restrict device SIM cards to only performing DFS related activities. Limit calls to the transaction device to originate from a few pre-authorized numbers of the provider. Agent call center to report fraud. To enable online transactions, use two-factor authentication. Each agent staff should have unique log in and password. Should employees be terminated, their passwords should be disabled.	Agent complaints
Customer requests reversal of valid transaction.	Customer requests cash out. Customer then denies receipt and requests provider to reverse transaction.	Any	A clear process to manage repudiation and ensure that the interests of all parties involved are taken care of. Transaction can be reversed, denied or put in to suspense until an investigation is completed. Agent education to report suspicious customer behavior.	High levels of recipient refusing to allow reversals
Agent defrauded by internal staff				
Provider employee defrauds agent	A provider employee uses unauthorized access to agent accounts in order to manipulate balances or conduct transactions to their own benefit.	Any	Carry out background checks of potential provider employees. Limit staff access to agent accounts. Use SMS receipts for agent transactions. Train agents on keeping PIN/login details secret.	Agent complaints

Risk	Description	Type of Institution	Policy Options & Potential Mitigation Tools	Key Risk Indicators
Instant commission fraud	For commission models that pay instant commission, business owners find it difficult to reconcile commissions earned as they become mixed up with other transactions. Employees take advantage of this mix up to defraud their employers.	Any	Provide digital information to facilitate agent reconciliation of transactions, cash and electronic float. Aggregation of commission payments to agents for payment after a scheduled period of time, preferably monthly. A report should be generated periodically specifying commission earned, the mode of payment and any reference number for the payment.	Agent complaints
Agent officer defrauds agents	Agents give their PINs away to the provider staff, giving them full access to the agent's float account.	Any	Educate agents to keep PIN confidential. Agent officer must ideally only have role-based rights and not login rights to access funds at the agent device.	Agent complaints
Agent defrauded by master agent				
Unauthorized withdrawal of agent funds or commission	Master agents carry out unauthorized withdrawal of funds from sub-agent's accounts or deduct commission.	Any	Detailed contracts and guidelines for operation of master agents regarding obligations, staffing, and requirements for sub-agent recruitment. Implement guidelines on commission sharing between master agents and sub-agents. Provide sub-agents with adequate feedback forums including hotlines, email addresses, and sub-agent forums to receive feedback. Detailed agent commission statements for agent reconciliation.	Agent complaints
Provider defrauded by customer				
Erroneous disbursements	Customers receive erroneous deposits of funds and withdraw funds and close accounts before funds can be frozen and returned.	Any	Organizations must develop a clear process for disbursement of funds to minimize errors. Comprehensive process that covers identification, monitoring, communication and management of fraud. Daily reconciliations of payments and receipts against internal systems.	Customer complaints
Provider defrauded by agent				
Split deposits	Agents split deposits in a number of smaller transactions in order to generate higher commissions at the cost of the provider.	Any	Use data analytics tools to flag suspicious transactions. Develop a comprehensive due diligence process for the recruitment of agents to minimize recruitment of agents with poor reputation or those likely to commit fraud. Carry out mystery shopping activities and practice good agent management. Education of agents. Call center for customers to report suspicious activity. Enforcement of penalties for agent mismanagement and closure of agents.	Suspicious transaction reports

Risk	Description	Type of Institution	Policy Options & Potential Mitigation Tools	Key Risk Indicators
Direct deposits	Agents deposit funds directly to a recipient's account - instead of to the customer's account followed by the customer conducting a P2P transaction - in order to bypass transaction fees.	Any	Carry out consumer education campaigns to create awareness about these types of fraud. Analyze and review agent commission structures regularly to detect any anomalies and address them. Mystery shopping to detect incidences of agent willingness to commit fraud. Use GSM network data to identify location of customer and agent to ensure that transaction is being conducted at the same location.	Suspicious transaction reports
Registration of fake accounts	Agents register fake accounts or customers without full KYC documentation in order to earn commission.	Any	Customer registration commission to be split between registration and first transaction. Back-office processing and compliance departments verify KYC. Commission paid on fully KYC'd accounts only.	Account registration rejection rates
Provider defrauded by outside party				
Hacking	An outside party hacks in to the system to gain access to provider accounts to perform fraudulent transactions or to steal data.	Any	Firewalls, encryption, role-based access rights, etc. Daily account reconciliation.	IT audit results
Provider defrauded by internal staff				
Ghost accounts	An employee uses unauthorized access to create fake accounts with fake deposits. Collusion with fraudsters allows them to withdraw funds from agent.	Any	Daily account reconciliation. Staff vetting and training. Adequate policies and procedures to investigate suspicious activity.	Internal audit IT audit results
Operational Risk				
Reconciliation and account variances	The risk that the actual value in trust accounts is different than amount reflected in system. Risk that off-net transactions (e.g. ATM withdrawal, bill payment) is not reconciled with internal accounts.	Any	For MNOs, system integration into bank accounts so all changes to main bank account is reflected automatically. Use separate accounts for business revenue and commission disbursement. End-of-day variance reports managed and signed off by appropriate business management. Robust system authority approver and checker function. Daily reconciliation at provider and agent. Robust internal policies and procedures for reconciliation of transactions in suspense accounts.	% of transactions in suspense accounts % end of day variance
Customer is unable to dispute a transaction or account charge.	Customers are not able to resolve disputes with an account provider and recourse to a government body or regulatory authority to arbitrate disputes is weak or non-existent.	Any	Efficient dispute resolution processes. Call centers are adequately staffed and trained with clear escalation policies for issue resolution. Clear, published, service standards.	Call center resolution rates.

Risk	Description	Type of Institution	Policy Options & Potential Mitigation Tools	Key Risk Indicators
Lost card or mobile phone	Customer is unable to transact due to lost debit card or SIM card.	Any	Card replacement policies. Call center for reporting and issue resolution. Agent training to provide first level customer service.	Card replacement rates PIN reset rates
Lack of operational manuals and business processes	Operating manuals are incomplete, lacking the exception processes and are not regularly updated resulting in poor operating procedures being followed	Any	Review operating manual against list of procedures being undertaken. Add any missing procedures, update existing procedures as required, and add the exception use cases to all. Ensure that relevant departments sign off each process. Create process checklists and ensure all processes have been documented and updated if required and circulated to relevant staff.	Internal Audit Risk & Compliance reviews Time taken to resolve disputes
Lack of operational audits	Current operational procedures are not optimized with regards to reconciliation and revenue processing.	Any	Risk audit needs to be performed to identify issues and ensure operational efficiency and integrity.	Internal Audit Risk and Compliance reviews
PIN resets	Lengthy or complicated PIN resetting procedures creates poor customer experience	Any	Efficient policies for PIN reset procedures	Time taken to resolve PIN resets
Debit without disbursement (DWD)	When an ATM debits a customer's account but does not dispense the corresponding cash causing delays in reimbursement to the customer.	Any using ATM enabled cards	Deepen relationships with interbank settlement systems for off-net transactions. Improve operational procedures for resolutions. Increase human resources dedicated to dispute resolution. Upgrade ATMs.	Number of incidents
Lack of internal controls, internal reporting and data monitoring	No procedures to monitor agent, employee or customer activity. Potential non-compliance with regulatory requirements.	Any	Implement internal controls to monitor entity and transaction activity through internal reporting and data monitoring.	Internal Audit Risk & Compliance Reviews
Reconciliation processes	Lack of effective reconciliation procedures creating backlogs.	Any	Have clear defined efficient reconciliation processes that are ideally automated.	% of unreconciled amounts Time taken to reconcile
Data input errors	Data input errors, typos, key stroke errors conducted by back office provider staff.	Any	Use maker and checker functions to perform tasks. Segregation of duties.	Reconciliation controls Internal Audit
Partnership Risk				
Relationship difficulties between the owners of the service – leading to service outage (for example in collaborations between FIs, MNOs, vendors and/or other service providers)	Significant relationship difficulty within the provider consortium results in service unavailability for customers.	Any	Detailed MOU with roles, responsibilities and clearly defined value proposition for each player in the partnership. Clear contractual arrangements for service continuity during disputes.	Internal audit results IT audit results

Risk	Description	Type of Institution	Policy Options & Potential Mitigation Tools	Key Risk Indicators
Unreliability of partners	Partners do not meet expectations and deliverables of agreements.	Any	Conduct due diligence on partners. Use performance guarantee contracts where payment is made upon sign-off. Invoke non-conformance penalties.	Internal audit scope results
Partner systems are down	Partner systems downtime disrupts service.	Any	Inform agents/customers via SMS when there are system downtimes as appropriate. Avail customer support lines. Use SLAs for partners to guarantee service uptime and apply non-conformance penalties. Develop back-up partners to spread the risk.	IT Audit results
Reputational Risk				
Fraud	Widespread fraud deters customer trust and creates reputational risk for provider and market as a whole.	Any	Limit fraud exposure. Proactive, prudent communications strategy for managing fraud exposure.	Fraud losses
Transaction failures	Transaction failures impact confidence in organization, and reduce client activity and retention.	Any	Improve technology / performance. Impose SLAs with vendors and partners. Customer education and marketing campaigns.	Transaction failure rates
MNO connectivity	Agents located in low connectivity areas disrupt customers access to services leaving customers frustrated and reducing trust in the provider.	Bank, MFI & PSP	Develop better relationships with the MNOs to enhance service quality. Use dual SIM devices with the two strongest MNOs in each particular area.	Volume of transactions in specific geographies
Poor customer experience	Poor customer support, untimely resolution of incidents, inability to contact provider.	Any	Incident resolution process and escalation matrix in place. Well-resourced customer care department.	Time to answer calls % of calls unanswered Call resolution rate
Brand risk from partnerships	Failure of partners to add value to provider's brand, and even to diminish brand based on poor reputation or quality of service.	Any	Customer communication and advertising campaign to develop brand. Develop multiple partnerships to reduce impact of one relationship.	Press reports on partner brands

Glossary

TERM	DEFINITION
Agent	A person or business contracted to process transactions for users. The most important of these are cash in and cash out (that is, loading value into the mobile money system, and then converting it back out again); in many instances, agents register new customers too. Agents usually earn commissions for performing these services. They also often provide front-line customer service, such as teaching new users how to complete transactions on their phones. Typically, agents will conduct other kinds of business in addition to mobile money. Agents will sometimes be limited by regulation, but small-scale traders, microfinance institutions, chain stores, and bank branches serve as agents in some markets. Some industry participants prefer the terms 'merchant' or 'retailer' to avoid certain legal connotations of the term 'agent' as it is used in other industries. (GSMA, 2014)
Agent banking	Banking services, often limited, carried out by an agent.
Alternative Delivery Channels (ADC)	Channels that expand the reach of financial services beyond the traditional branch. These include ATMs, Internet banking, mobile banking, e-wallets, some card /POS device services, and extension services.
Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT)	AML/CFT are legal controls applied to the financial sector to help prevent, detect, and report money-laundering activities. AML/CFT controls include maximum amounts that can be held in an account or transferred between accounts in any one transaction, or in any given day. It also includes mandatory financial reporting of KYC for all transaction in excess of $10,000, including declaring the source of funds, as well as the reason for transfer.
Automatic Teller Machine (ATM)	An electronic telecommunications device that enables the customers of a financial institution to perform financial transactions without the need for a human cashier, clerk, or bank teller. ATMs identify customers via either a magnetic or chip-based card, with authentication occurring after the customer inputs a PIN number. Most ATMs are connected to interbank networks to enable customers to access machines that do not directly belong to their bank, although some closed-loop systems also exist. ATMs are connected to a host or ATM controller using a modem, leased line or ADSL.
Application Program Interface (API)	A method of specifying a software component in terms of its operations by underlining a set of functionalities that are independent of their respective implementation. APIs are used for real-time integration to the CBS/MIS, which specify how two different systems can communicate with each other through the exchange of 'messages'. Several different types of APIs exist, including those based on the Web, TCP communication, and direct integration to a database, or proprietary APIs written for specific systems.
Call center	A centralized office used for the purpose of receiving or transmitting a large volume of requests by telephone. As well as handling customer complaints and queries, it can also be used as an alternative delivery channel to improve outreach and attract new customers via various promotional campaigns.
Channel	The customer's access point to a financial service provider, namely who or what the customer interacts with to access a financial service or product.
Digital Financial Services (DFS)	The use of digital means to offer financial services. Encompasses all mobile, card, POS, and e-commerce offerings delivered to customers via agent networks.
Electronic banking	The provision of banking products and services through electronic delivery channels.
Enterprise Risk Management (ERM)	The process of planning, organizing, leading, and controlling the activities of an organization in order to minimize the effects of risk on an organization's capital and earnings.
e-money	Short for 'electronic money', it is stored value held in accounts such as e-wallets or on cards. Typically, the total value of e-money issued is matched by funds held on one or more bank accounts and usually held in trust, so that even if the provider of the e-wallet service was to fail, users could recover the full value stored in their accounts.
E-wallets	An e-money account belonging to a DFS customer and accessed via mobile phone.

Financial Institution (FI)	A provider of financial services including credit unions, banks, non-banking financial institutions, microfinance institutions, and mobile financial services providers.
ISO 31000	ISO guidelines established for the implementation of Enterprise Risk Management (ERM).
Key Risk Indicator (KRI)	A Key Risk Indicator is a measure used to indicate how risky an activity is. It differs from a Key Performance Indicator (KPI) in that the latter is meant as a measure of how well something is being done, while the former indicates how damaging something may be if it occurs and how likely it is that it will occur.
Know Your Customer (KYC)	Rules related to AML/CFT that compel providers to carry out procedures to identify a customer and that assess the value of the information for detecting, monitoring, and reporting suspicious activities.
Master Agent	A person or business that purchases e-money from a DFS provider wholesale and then resells it to agents, who in turn sell it to users. (Unlike a super-agent, master-agents are responsible for managing the cash and electronic-value liquidity requirements of a particular group of agents.)
Merchant	A person or business that provides goods or services to a customer in exchange for payment.
Microfinance Institution (MFI)	A financial institution specializing in banking services for low-income groups, small-scale businesses, or individuals.
Mobile banking	The use of a mobile phone to access conventional banking services. This covers both transactional and non-transactional services, such as viewing financial information and executing financial transactions. Sometimes called 'm-banking'.
Mobile money service/ mobile financial service (MFS)	A DFS that is provided by issuing virtual accounts against a single pooled bank account as e-wallets, that are accessed using a mobile phone. Most mobile money providers are MNOs or PSPs.
Mobile Network Operator (MNO)	A company that has a government-issued license to provide telecommunications services through mobile devices.
Point of Sale (POS)	Electronic device used to process card payments at the point at which a customer makes a payment to the merchant in exchange for goods and services. The POS device is a hardware (fixed or mobile) device that runs software to facilitate the transaction. Originally customized devices or PCs, but increasingly include mobile phones, smartphones, and tablets.
Risk Assessment	The process of identification, evaluation, and mitigation strategy development of risks.
Risk Management Framework	A comprehensive set of policies aimed at reducing the impact of risks associated with DFS. The framework is a culmination of all planning and assessment processes and includes the risk register as its main body and working document.
Risk Register (Risk Matrix)	The central database of identified risks, along with their descriptions, causes, effects, and policies - whether it is to tolerate, treat, transfer, or terminate.
Short Message Service (SMS)	A 'store and forward' communication channel that involves the use of the telecom network and SMPP protocol to send a limited amount of text between phones or between phones and servers.
Smartphone	A mobile phone that has the processing capacity to perform many of the functions of a computer, typically having a relatively large screen and an operating system capable of running a complex set of applications with Internet access. In addition to digital voice service, smartphones provide text messaging, e-mail, web browsing, still and video cameras, an MP3 player, and video playback with embedded data transfer/GPS capabilities.
Super-Agent	A business, sometimes a bank, which purchases electronic money from a DFS provider wholesale and then resells it to agents, who in turn sell it to users.
Unstructured Supplementary Service Data (USSD)	A protocol used by GSM mobile devices to communicate with the service provider's computers/network. This channel is supported by all GSM handsets, enabling an interactive session consisting of a two-way exchange of messages based on a defined application menu.

References

1. Risk Management Toolkit, GSMA & Consult Hyperion, 2015 (http://www.gsma.com/mobilefordevelopment/managing-risk-in-mobile-money-a-new-comprehensive-risk-toolkit)

2. MMU Managing the Risk of Fraud in Mobile Money, GSMA, 2012 (http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/10/2012_MMU_Managing-the-risk-of-fraud-in-mobile-money.pdf)

3. Mobile Financial Services Risk Matrix, USAID and Booz Allen Hamilton, 2010 (http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/06/mobilefinancials-ervicesriskmatrix100723.pdf)

4. Bank Agents: Risk Management, Mitigation, and Supervision, CGAP, 2011 (http://www.cgap.org/publications/bank-agents-risk-management-mitigation-and-supervision)

5. Digital Financial Services Risk Assessment For Microfinance Institutions, A Pocket Guide, AFI, 2014 (https://lextonblog.files.wordpress.com/2014/09/dfs_risk_guide_sept_2014_final.pdf)

6. Mobile Financial Services Technology Risks, AFI, 2013 (http://www.afi-global.org/sites/default/files/pdfimages/AFI_MFSWG_guidelinenote_TechRisks.pdf)

7. Fraud in Mobile Financial Services, Mudiri, Microsave, 2012 (http://www.microsave.net/resource/fraud_in_mobile_financial_services#.VmWI9E10xes)

8. Risk Management in Mobile Money, Lake, IFC, 2013 (http://www.ifc.org/wps/wcm/connect/37a086804236698d8220ae0dc33b630b/Tool+7.1.+Risk+Management.pdf?MOD=AJPERES)

9. Enterprise Risk Management (ERM) and the requirements of ISO 31000, AIRMIC, Alarm, IRM, 2010 (https://www.theirm.org/media/886062/ISO3100_doc.pdf)

Lesley Denyes

Lesley is a Digital Financial Services Specialist with the IFC who has worked in the sector for over fifteen years, specifically in the areas of business modelling, financial analysis, mobile banking, strategic planning, product development and channel management in Asia and Sub-Saharan Africa. Lesley has worked with commercial banks, mobile network operators, payment service providers, research institutes, mobile app developers, NGOs, and consulting companies to reach low income households through technology and branchless banking. She is based in Toronto, Canada, and has a BSc in Quantitative Economics from Dalhousie University, Canada, and an MBA from Edinburgh Business School, UK.

Susie Lonie

Susie spent three years in Kenya creating and operationalizing the M-PESA mobile payments service, after which she facilitated its launch in several other markets including Tanzania, South Africa and India. In 2010 Susie was the co-winner of "*The Economist Innovation Award for Social and Economic Innovation*" for her work on M-PESA. She became an independent DFS consultant in 2011 and works with banks, MNOs, and other clients on all aspects of providing financial services to the unbanked in emerging markets, including mobile money, agent banking, international money transfers, and interoperability. Susie works on DFS strategy, financial evaluation, product design and functional requirements, operations, agent management, risk assessment, research evaluation, and sales and marketing. Her degrees are in Chemical Engineering from Edinburgh and Manchester, UK.

The Partnership for Financial Inclusion

The Partnership for Financial Inclusion is a $37.4 million joint initiative of IFC and The MasterCard Foundation to expand microfinance and advance digital financial services in Sub-Saharan Africa. The Partnership is also supported by the Bill & Melinda Gates Foundation and the Development Bank of Austria (OeEB, Oesterreichische Entwicklungsbank.AG). It works with microfinance institutions, banks, mobile network operators and payment service providers across the continent to test and evaluate innovative business models for financial inclusion. The program has a strong knowledge sharing component. This handbook is the second in a series of handbooks on how to successfully implement digital financial services, and one of many knowledge publications of the Partnership. For further information and to access all reports, please visit www.ifc.org/financialinclusionafrica

About IFC

IFC, a member of the World Bank Group, is the largest global development institution focused on the private sector in emerging markets. Working with more than 2,000 businesses worldwide, we use our capital, expertise, and influence, to create opportunity where it's needed most. In FY15, our long-term investments in developing countries rose to nearly $18 billion, helping the private sector play an essential role in the global effort to end extreme poverty and boost shared prosperity. For more information, visit www.ifc.org

About The MasterCard Foundation

The MasterCard Foundation works with visionary organizations to provide greater access to education, skills training and financial services for people living in poverty, primarily in Africa. As one of the largest, independent foundations, its work is guided by its mission to advance learning and promote financial inclusion to alleviate poverty. Based in Toronto, Canada, its independence was established by MasterCard when the Foundation was created in 2006. For more information and to sign up for the Foundation's newsletter please visit www.mastercardfdn.org.

CONTACT DETAILS

Anna Koblanck

IFC, Sub-Saharan Africa

akoblanck@ifc.org

www.ifc.org/financialinclusionafrica

2016

The MasterCard Foundation

IFC International Finance Corporation WORLD BANK GROUP