10.31341/jios.46.1.6
Open Access
UDC 004.056:336.71(676.1)
Original Scientific Paper

Towards an Improved Framework for E-Risk Management for Digital Financial Services (DFS) in Ugandan Banks: A Case of Bank of Africa (Uganda) Limited.

Andrew Arim *andrew.arim@cancom.de*
CANCOM Public GmbH
Granatenstrasse, 19-20, Berlin, 13409, Germany

Joseph Wamema *jwamema@umu.ac.ug*
African Centre for Agroecology and Livelihood Systems
Uganda Martyrs University, Kampala, 5498, Uganda

Abstract

One of the predominant challenges facing banks in low resource countries is the management of Digital Financial Services (DFS) risks. Many banks are making worthwhile efforts to boost the factors that make them come on top of the challenges, unfortunately they have fallen short. This article sought to develop an e-risk management framework for DFS in Ugandan banks. Design Science Research paradigm, a mono-method qualitative research method and a case study research strategy was adopted. Questionnaires, interviews and document review were the main data collection methods. Findings from this study indicate that banks in Uganda use a handful of DFS business models and face a number of DFS risks including; talent for DFS, technology, strategy, governance, product, client acquisition, crime/fraud, regulation, and agent management among others. Notwithstanding, Ugandan banks should carefully balance IT spend across customer expectations, improve cybersecurity and internal process and regularly check its IT security.

Keywords: E-Risk, Digital Financial Services, Digital Risk Management, Bank Risk Management, Information Security, Cybersecurity

1. Introduction

The importance of Digital Financial Services (DFS) in creating a more inclusive, stable and secure financial sectors globally cannot be over emphasized. Today, the growth in mobile telecommunication service availability is expanding the reach of financial services across wireless networks in low resource countries—Uganda inclusive, creating the potential for significant growth in financial inclusion. While the benefits of DFS are easily identifiable, grave concerns have emerged with respect to the risks that users of these services are likely to face. Several researchers and practitioners have observed that the risks that are inherent in all retail payment systems

including; money laundering, privacy and security, consumer protection, fraud, and credit and liquidity risks are also present in the digital space [23], [24], [7], [25].

With evidence of a large number of nonbank participants in the delivery of DFS, such as Mobile Network Operators (MNOs) and their agents, as well as the technology vendors, there is likely to be additional risk considerations for banks. Against this backdrop, it implies that, as DFS evolve, there are numerous issues that need to be considered in managing the risks that wireless payment systems may introduce; and given the unique experience of the growth of DFS most especially in emerging markets and low resource countries, the need to solve every day lived experiences and challenges is inevitable. It is essential that the risks that can occur via the use of digital technologies in financial service delivery be recognized by all stakeholders and measures be put in place to ensure that problems do not arise. This study therefore aims at designing a comprehensive e-risk management framework for DFS delivery in banks which will also help in addressing any possible confusion and problems in existing regulation vis-a-via emerging trends in DFS delivery.

2. Background

Globally, the providers of financial services for commercial reasons are rapidly matching towards the digital age, by partnering with MNOs and/or other payment service providers. This can be exemplified in Pakistan where Tameer Bank in Pakistan in cooperation with its telco owner Telenor expanded payment services leading to significant growth in transaction fee income. On the other hand, MFIs (Microfinance Institutions) including Musoni in Kenya, are establishing digital field applications in order to alter traditional banking business models [1]. DFS are on course to be strong tool in the establishment of a more secure, stable and inclusive financial sectors. Today, a significant section of the bankable population in the world still live outside the formal financial system. In reference to the World Bank report of 2014, Global Financial Inclusion (Global Findex) database, about 38 percent of people above 18 around the world do not have an account at a conventional financial institution or mobile money provider.

In Uganda, the market for DFS is at present marshaled by MNOs, and the main operant MTN and Airtel overseeing the vast majority of transactions and users [3], [25]. In order to remain competitive, a number of banks have entered into strategic partnerships with these MNOs to provide financial services to their customers. A number of these cooperation are two-way relationships leading to inadequacy and frailty in the payment systems.

The growth of the digital economy comes with an array of associated disbenefits. The ramification is on end users, workers, and businesses and could be translated as part and parcel of unfavorable inclusion and blend into digital markets, with increased indebtedness as the digital economy heightens, resulting to persistent incidents of security breaches targeting shared interests of businesses, national governments, and end users [17]. As reiterated by [10], the most exposed to such security issues are low resource countries, because they are portrayed and seen as an “ideal testing ground” by hackers for the most grievous attacks. Due to the weak infrastructure for security

in low resource countries, hackers are in position to evade detection and they always use these vulnerabilities to experiment their malware before making use of it against more polished defenses. Examples include hackers stealing billions of shillings in a mobile money heist from Ugandan banks and telecom companies-MTN (Mobile Telecommunications Network) and Airtel [12], defrauding of US$4m from financial accounts in Zambia [21], or hackers stealing US $81m from the Bangladesh bank [28].

As DFS evolve, there are numerous issues that need to be considered in managing the risks that wireless payment systems may introduce. The multiple regulatory domains governing banking and telecommunication in most of the low resource countries today, Uganda inclusive, has been accustomed to operating autonomously from one another and is likely to be challenged to learn how to effectively cooperate to provide oversight for DFS [8]. According to [19], some of the risks stem from demand-side factors, such as limited consumer digital literacy, unfamiliarity with formal finance, and issues of financial capability.

Given the unique experience of the growth of DFS most especially in emerging markets, the need to solve every day lived experiences and challenges is inevitable. It is essential that the risks that can occur via the use of digital technologies in financial service delivery be recognized by all stakeholders and measures be put in place to ensure that problems do not arise.

2.1. Digital Financial Services, Risk and e-Risk Management

Risk is described as the 'effect of uncertainty on objectives'. An effect is a departure from the anticipated—positive and/or negative [11]. Risk is described by [20] as 'the likelihood for loss or misstep to meet business objectives as a result of internal or external events'. An e-Risk is defined as the likelihood of a vengeful electronic event; whose happening causes loss to e-business. These comprises of: (i) Identity theft, (ii) Destruction or compromise of perimeter network security components, (iii), Denial of Service (iv) Application or Internet Service Provider failing, (v) Graffiti, (vi) Cyber-extortion and fraud, (vii) Attack by wireless devices, (viii) Attacks by disgruntled employees, among others.

2.1.1. DFS delivery Infrastructure and Ecosystem

According to two DFS supporting organizations, vendors in the market offer DFS tenets [26]. The vendors and operators majorly comprises of MNOs and banks but can also encompass value-added service providers, third-party service providers, and juxtaposed players such as retailers and other enterprises. Being guided by regulators, providers do offer services to the market and get involve in market share competition, by part of the time getting involved in partnerships and 'co-opetition'. Providers are hereby designated into three main classes: Banks, MNO and third-party operators.

2.1.1.1 DFS Technology Components

DFS uses a combination of four elements as a technology platform, these include a physical device, an application – this runs on the device to be used in providing DFS,

a channel for communication – data interchange between the device and the service provider's host system occurs through the communication channel, and last but not least, the mode of authentication – this is used to approve the identity of the channel user.

2.1.1.2 DFS Ecosystem

A stereotypical ecosystem for DFS comprises of end users (businesses, government agencies, consumers, and NGOs) [4]. They present demand for digital and interactive financial products and services. The actors that include banks, non-banks, and other licensed financial institutions come up with those products and services digitally and the financial, technical, and other infrastructures provide the possibility of those products. The qualification and fitness for use and operation are provided by governmental policies, laws and regulations that allow them to be delivered in an attainable, inexpensive, and safe manner.

2.1.2. DFS delivery models and channels

A business model is referred to as a visionary framework used by businesses to present a fundamental economic logic and system that presents a picture and proof of how a business can deliver value to customers at a reasonable cost and make profit out of it [27]. E/M-Banking business model revolves around nine (9) building blocks [18], [15], p. 8-10). These are: 1) Revenue streams; 2) Value propositions; 3) Key activities; 4) Customer relationships; 5) Customer segments; 6) Key resources; 7) Channels; 8) Key partnerships; and 9) Cost structure. According to [2], there are around six (6) DFS delivery models; Bank-based model, Bank-led model, Non-bank-based model, Payment Services Provider (PSP), Third-party provider, MNO/bank model, and Government Provider/Bank Model.

DFS delivery channels can be self-service or Over the Counter (OTC), whereby the customer interacts with staff or third party representatives such as an agent or merchant—which is dedicated or not. The categorization of a channel as either OTC or self-service becomes somewhat cumbersome when it comes to issues such as e-wallets because these channels habitually needs some level of interaction of OTC to cash in/out and then it can be used afterwards in self-service mode. The channels include; ATM, Internet banking, Agent/Merchant, Extension services (field staff, mini branch, branch on wheels), Mobile banking, E-wallet (m-wallets, prepaid cards, store cards), and Call center.

2.2. DFS delivery challenges and risks

The following are the challenges and risks associated with DFS delivery, as noted by [6], [9]. It should be noted that some of these challenges and risks are associated to the aforementioned DFS delivery models and channels and others are not. They include: Human error, Strategic risk, Regulation, Operational Risk, Technology, Financial Risk, Political risk, Agent management, Fraud, Reputation, Partnership,

Talent, Governance, Product risk, Service delivery, Management, Crime, Competition, Client acquisition, and Funding among others.

2.2.1. DFS risk mitigation requirements

There are many requirements that needs to be met by DFS providers in order to mitigate DFS risks, some of which are presented by [2], [9] as follows: Agent Due Diligence (ADD), Biometric Identification System, Know Your Customer (KYC), Risk-based Approach, Business Processes, Adequate Internal Control System, Adequate Internal Audit, Segregation of duties, Adequate External Reporting, Adequate External (Financial) Audit, Execution, Delivery and Process Management, Reconciliation and Account Variances, Agent Management Excellence, Deposit Insurance, and Trust Accounts.

2.3. Risk Management Frameworks and DFS Best Practices

In this sub-chapter, a description, analysis and review of the two (2) commonly used RMFs (Risk Management Frameworks) are given, these are: 1) ISO 31000:2018 RMF, and 2) NIST SP 800-37:2018 RMF for Information Systems and Organizations.

2.3.1. ISO 31000 Risk Management Framework 2018

ISO 31000 was originally published in 2009. An updated version was published in February 2018. Nonetheless, the overarching goal of ISO 31000 is still the same – that is, integration of risk management into a strategic and operational management system. It should be noted that the risk management principles and the framework are related intimately. Version 2018 is very much similar to the original version (2009), except for the following changes: 1) risk management principles have been reviewed, as these are the key criteria for successful risk management; 2) the importance of leadership by top management is strongly emphasized, as well as the integration of risk management, beginning with the governance of the Organisation; 3) a lot of emphasis is placed on the iterative nature of risk management, as new knowledge and analysis leads to revision of processes, actions and controls; and 4) the sum and substance of the RMF is faired with a great focus on constantly holding up an open systems model to fit multiple needs and contexts. ISO 31000-2018 encompasses much treasured information and it representing a robust and high-level guideline for the management of risk. It asserts that the purpose of risk management is the creation and protection of value. In summary, ISO 31000 locates greatly, an emphasis on understanding the Organisation and its context.

2.3.2. NIST RMF for Information Systems and Organizations 2018

NIST SP 800-37: 2018—RMF for Information Systems and Organisation was released in December 2018. The RMF lays bare parameters for putting into practice the RMF to information systems and organizations. The Framework provides a

disciplined, structured, and flexible process for managing security and privacy risk from two angles—an information system angle and a common controls angle and is "purposefully mapped-out to be technology neutral in a sense that the methodology can be applied to any type of information system without modification". The RMF also emphasizes "automation" wherever necessary and possible to increase the speed, effectiveness, and efficiency of executing the steps in the RMF. It further requires organizations to modernize their IT infrastructure and systems and recognizes the increasing interconnectedness of information systems and networks. The RMF consist of seven (7) steps; a preparatory step to ensure that organizations are ready to execute the process and six main steps: Categorize; Select; Implement; Assess; Authorize; and, Monitor.

2.4. Design requirements (criteria) for quality and updated RMF

Requirements serve not only to describe what to build and why it is being built but also provide a way to measure whether an activity has been successful [5]. The first step in developing an updated DFS e-RMF (e-Risk Management Framework) approach is to capture a set of design requirements/criteria (derived from literature review and classroom experience). Thirteen (13) requirements are hereby put forward to guide the Framework design efforts as listed and described in Table 1.

Requirement	Description
1. Purpose and Scope	The framework should be new, interesting, and true. There should be enough information to argue that the RMF is new and interesting to the relevant research and practice community.
2. Business and Technology Awareness	The framework should take both business and technology into consideration.
3. Ease of Use	The framework should be understandable among different user groups, such as within members of risk management, IT, DFS channel management, Agency banking, sales and marketing, finance, internal control and compliance, management of the bank, as well as external experts, consultants, and facilitators.
4. Genericity	The framework should be adaptable to different banks and risk situations and environments. The RMF should provide for evolution, adaptation, or learning of any resulting artifacts without affecting the RMF. The RMF should have a degree of permanence and range of coverage so that one does not have to create a new version of the RMF for each new situation.
5. Layered Structure (abstraction)	The framework should prefer abstraction in order to hide unnecessary details. The RMF should not loose meaning when changed in any way.

6. Modularity	The framework should consist of different parts or modules that could be combined in different ways.
7. Reusability	The framework should be reusable in order to be adaptable into different risk situations.
8. Concepts, Tools and Technique Neutrality	The framework should support different risk management concepts, tools, technique, and platforms.
9. Constructs	All the existing and new concepts and entities that are needed to fully understand a RMF should be fully described.
10. Principles of Implementation	There should be a clear cut description of the process for instantiating and/or implementing a RMF.
11. Justificatory knowledge	There should be references to justificatory-knowledge tacit theory (such as informal experience-based insights and intuitions) that can provide a reasonable degree of justification of the framework. There should be insights provided into why one should believe in the framework.
12. Evaluation and Validation propositions	There should be a clearly stated description of how a RMF should be evaluated/tested for truthfulness, usability, efficacy, and quality. There should be artifact meta-requirements, meta-design, and evaluation criteria and measures.
13. Knowledge of Form and Function	There should be a clear explanation of how a RMF contributes/has contributed to the body of knowledge.

Table 1: DFS e-RMF Design Requirements (criteria)

2.5. DFS best practices

Below are the five basic steps that should be taken to manage risk in the digital environment [29]: Step 1: Risk Identification; Step 2: Risk Analysis; Step 3: Risk Evaluation; Step 4: Risk Treatment; and Step 5: Risk Monitoring and review. It should additionally be noted that, for proper and safe delivery of DFS, providers need competencies in; Information and Cyber Security; Resilience and disaster recovery; Vendor and third party management; Project and change management; Architecture development and testing; Data quality and governance; and finally, ICT compliance [13].

3. Methodology

This study adopted the Design Science Research paradigm, a mono-method qualitative research method and a case study research strategy. Research was realized between March-June 2020 by collecting data from employees of one Ugandan bank and industry practitioners. Questionnaires, interviews and document review were the

main data collection methods. Data analysis was conducted using Colaizzi's (1978) framework for qualitative data analysis. Focus group interview and engagement with the field were incorporated into the data collection and analysis. The test-retest, triangulation, and 'thick description' methods were employed in this study and the design of the questionnaires and interview guides was based on literature from previous similar and/or related studies, all in an endeavor to ensure validity and reliability.

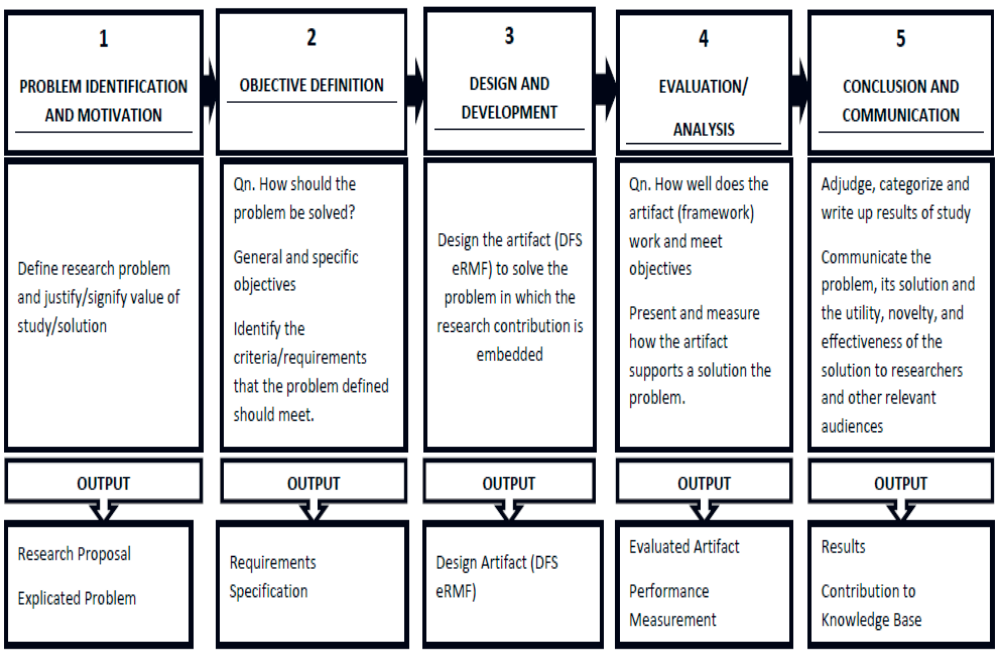

Figure 1: DFS e-RMF design process with outputs at every stage

4. Results

The rate of response to the researcher's requests for interviews with various selected participants was fairly good. Within the bank, the number of participants proposed was nearly achieved, with the exception that more department and functional managers were found willing and available to be interviewed than had been planned while a fewer number of lower level employees participated than originally proposed. Among the banking industry experts, consultants, and facilitators, only three out of the six proposed were eventually interviewed. This was found to be helpful within a case study because the various interviewees came from different departments/designations and they displayed somewhat different and varied responses to DFS risk and risk management.

Category	Office/Department/Designation	Estimated Population	Proposed Sample	Actual Response
Bank Employees (#BOA)	**Management**	**8**	**6**	**5**
	Agency banking	2	2	2
	IT	2	1	1
	Customer Care	2	1	1
	Finance	2	2	1
	Other Staff	**12**	**10**	**7**
	Agency banking	8	2	2
	IT	6	2	1
	Sales and Marketing	5	1	1
	Finance	5	1	1
	Compliance	4	2	1
	Customer Care	5	2	1
Banking Industry Practitioners (#BIP)	**Consultants, Experts, & Facilitators**	**8**	**7**	**5**
	DFS Specialist	3	2	2
	Financial Inclusion Consultant	2	2	1
	Uganda Bankers' Association	3	2	2
Total		**28**	**22**	**17**

Table 2: Proposed and Actual Participants and Respondents

4.1. Emerging themes from Interview data

The thematic and content analysis performed on the interview manuscripts produced a number of themes discussed below. Overlaps will be found between some of the themes. All the themes are discussed in 2 categories of respondents, i.e. bank staff (both management and other employees) and banking industry practitioners (experts, facilitators, and consultants).

4.1.1. DFS delivery models, challenges and risks of Ugandan bank

The bank has a fairly robust DFS/mobile banking technology platform available providing seamless and real-time access between, for example, a mobile phone and a bank account and a fairly mutually aligned DFS business model and synchronized DFS strategy.

The bank has already forged strategic multi-industry alliances to offer DFS to the un/underbanked segment. Rapid technological innovations, evolving DFS delivery models and state initiatives such as National ID programme have greatly facilitated the improvement of DFS conditions at the bank and the bank is considering building self-sustaining DFS alternatives to extend banking and other financial services to the excluded.

4.1.1.1 DFS delivery models and channels of Ugandan banks

Bank Employees

The bank runs the following models of DFS delivery: 1) option "b" of the bank-based DFS model where the bank is licensed or otherwise permitted by the regulator to provide DFS, 2) Bank-led model— the bank is the primary driver of the product or service. The bank manages all angles of marketing, branding and customer relationship management, 3) Payment Services Provider (PSP)—the bank provides services enabling funds to be deposited and withdrawn from an account. The bank also performs payment transactions that involves transfers of funds, issuance of payment instruments such as checks, e-Money, credit cards and debit cards, and remittances and other services central to the transfer of funds, 4) Third-Party Provider—the bank uses agents to act on their behalf pursuant to a services agreement and other contractual arrangement and the bank is liable for the actions of the third-party providers acting on their behalf, and finally.

The bank uses extension services and agency banking as DFS delivery channels. For the purpose of this study, the researcher needed to differentiate between the two. While agency banking relies on use of third-party operators, extension services involves equipping the bank staff with technology solutions. The bank also provides DFS through technology and technical interface including ATM, web and USSD interfaces accessible through smart/mobile handsets.

Other channels the bank uses in delivering DFS includes Internet banking, Extension services, Mobile banking, and E-wallet. The bank also operates a call center that is used for receiving and transmitting requests through telephone and handling customer complaints and queries.

The bank reported having full control of most of the sections of the DFS value chain including user accounts and brand, the communication channels like data and USSD (except for SIM which is partly shared with the telecoms), physical channels like agents and ATMs. The bank also controls user/transaction data.

The bank's financial infrastructure consists of payment clearing and settlement systems, which enable the processing of various types of payments. In this environment, the mobile network operator provides both ICT infrastructure and an agent network, while the bank provides both payment services and payment infrastructure.

Banking Industry Practitioners

DFS implementations by Ugandan banks employ many delivery approaches and use different terminologies, such as 'e-banking' and 'branchless banking'. Modern technologies are being implemented by these banks leading to quite a number of benefits.

Respondents also noted that banks in Uganda use a combination of delivery channels in executing DFS. An overlap clearly exists wherein banks may sometimes opt to use non-bank services as one of their delivery channels, such as when banks are linked to e-wallets services.

4.1.1.2 DFS delivery challenges and risks of Ugandan banks

Bank Employees

Strategically, bank management is lacking in fully investing in DFS resources for targets to be met. "DFS operations here is understaffed, marketing is under-resourced and the bank sometimes fails to meet targets for customer acquisition and activation" noted one respondent. Sometimes de-prioritization of DFS products and channels is a result because of poor performance leading to the bank reorienting around competing priorities. Competitors are also gaining market share owing to superior service or lower prices.

There was concern about management risk – this touches on several points, including the quality of management, the availability of talent, the incentives offered to management, and the ability of management to handle this atmosphere of rapid technological change. Many respondents blamed poor management on inappropriate qualification, inexperience or sheer incompetence.

Client acquisition is a big problem. Getting DFS out to rural areas poses a rather special challenge. Most Ugandan villages are too remote, largely illiterate, subject to particular risks (such as weather and floods), and unattractive to DFS suppliers who mostly have short-term profit goals. As respondent #BOA06 pointed out, "many people don't have electricity or even ID leave alone National ID documents".

Respondent #BOA03, reported that "the extent of transactions assisted by agents have exposed inexperienced customers to risks, in a case where agents and their employees have insufficient capacity, training, and support or are dishonest".

ATMs and other digital interfaces used by the bank is also known to present a lot of problems. Respondent #BOA04 reported: "Many of our DFS consumers are first-time users of formal finance and background and they sometimes struggle with issues like language barriers, complicated interfaces, and systems of many operational steps (multi-step processes) ... this is because most are using phones with basic feature having limited interface options."

The ICT security officers consulted in the bank and banking sector told the interviewer they are challenged by identifying assets across the bank and keeping track of their status and configurations, including hardware and software. This boils down to Enterprise Architecture failure.

DFS systems at the bank is sometimes unavailable and customers cannot access their accounts or their transactions can fail due to this. Customers sometimes fail to access account through an application or agent due to the bank's system experiencing temporary system downtime or because of the unavailability of a mobile network. Other technological risks affecting the bank sometimes but not all the time includes; malwares, transaction delays, hardware failures, loss of data, and failure of DFS hosting environment.

There is a lack of "data intelligence" that is supposed to draw on data management, data science and cybersecurity tools to verify data from its origin through its full life cycle, and scrutinize how it is used to make DFS risk decisions and ensure that it is safely and securely stored.

The bank is also employing very limited tools in managing risk and yet the bank management are increasing their focus on risk management as an emerging core competency, and most of them see the need for better data and information, so the bank can take action on an ever-evolving inventory of DFS risks. One challenge risk managers at the bank face is that risk data is scattered across the organization and not shared across business unit silos and there are no specific tools to help in solving these challenges.

Further to the risks, there is a problem with agent management being faced by the bank. This includes poor communication by network agents, lack of agent liquidity, agent inactivity, agent unavailability, poor quality customer experience at agents and agent business case.

Banking Industry Practitioners

The country's banking sector faces underdeveloped technology and venture capital ecosystems - shortage of skilled tech/finance people and entrepreneurs, small markets, and limited revenue potential of citizenry. There is a relatively weak infrastructure such as underdeveloped payment systems, customer credit data, legal enforcement mechanisms for payment obligations, power, and telco/Internet coverage.

Ugandan banks see the arrival of new technology posing the greatest risk to their business because of its complexity, the high cost of investment involved and the enormous changes it is bringing to financial services. Many banks have reported the same issue and that is-failure to master new technology could mean elimination from the market. Inability to transact due to unreliable network/service (network downtime) is logged as one of the top customer concern.

Ugandan banks face the risk of partnership. Developing, establishing, and overseeing an inclusive DFS ecosystem involves engagement with a more diverse and larger group of actors and stakeholders. This is needed in two domains: a) stakeholder management and b) infrastructure management of which most Ugandan banks are having problems executing successfully.

A lot of technology issues have been reported in Ugandan banks such as complexity of the interface for the DFS clients (ergonomics) - The level of literacy or the poor ergonomics of the DFS applications (commercial or client) impacts the ability of the clients/customers to master the different platforms; Missing features - The platform is sometimes limited in functionality, negatively impacting transactions or interactions with the clients; Web front poor ergonomics - In some cases, banks do not fully understand its target market for DFS as reported by a respondent ‘sometimes there is an incorrect understanding of the customer which leads to development of products and channels not suited for the target customer’.

Competition as a result of changes in the market are pitting different types of institution in Uganda against each other – FinTech companies, commercial banks, MFIs – with different strengths and weaknesses. Respondent #BIP01 noted "Many Ugandan banks feels the playing field on which they operate is not level. Banks has got greater liquidity, FinTechs possess the technical know-how, commercial groups such as DFS suppliers are after profits, microfinance lenders see themselves playing a social role".

Finally, the supersonic speed of innovation and technological/platform change greatly affects the DFS channel strategies. Respondent #BIP05 noted that "the rapid speed of innovation and technological change has affected the Ugandan banking industry by making DFS strategies redundant and obsolete before a technology/platform and/or innovation is used."

4.1.2. DFS risk mitigation requirements of Ugandan banks

4.1.2.1 General DFS risk mitigation requirements

Bank Employees

The bank uses incident investigation, auditing, and Internal communication and Periodical reports in identifying DFS risk. From this view, it can be noted that the bank leaves behind very important DFS risk identification approaches including Industry benchmarking, risk survey, Inspection by the bank risk staff, Incident investigation, and brainstorming. The bank is however making progress on ideas and solutions to reduce customer related DFS risks such as operational risks and is endeavoring to improve the awareness and ability of customers to avoid DFS risks. The bank reports of planning to spend a reasonable amount in their budget towards digital transformation.

The bank uses Know Your Agent/Customer (KYA/KYC) also sometimes known as Customer/Agent Due Diligence (CDD/ADD) methodologies to ensure they understand and know their customers and agents. Internal and external audits are carried out by the bank in an endeavor to manage risk.

Digitization of core business functions and processes is being taken by the bank including the digitization of sales and marketing, human resources, IT, etc. However, there is limited and less efficient risk management information systems in place and yet the standard goes 'as banks digitize, so must risk and treasury' because it is becoming increasingly common that banks are no longer "owning" the client interface because of digitization.

Traditional risk management frameworks are being used by the bank-to be specific, ISO 31000 even in managing DFS related risks like operation and credit risk. This is important although the complexity comes in situation where there are unique risks being brought about by digitization and DFS.

Banking Industry Practitioners

Most Ugandan banks are considering the use of biometric devices to reduce fraud. They are adopting policies and procedures to enhance fraud detection such as on utilization of PINs and conducting customer education on PIN protection. While the bank and the banking industry actors still lack the full picture on DFS risks and risk management, they are becoming increasingly aware of them and the need to improve mitigation.

4.1.2.2 Information/DFS Systems risk mitigation requirements

Bank Employees

Security Operations Management: This is the on-the-ground process by which security incidents at the bank are managed, security controls are implemented and maintained, and people with a higher level of access to IS/DFS systems and data are subject to oversight.

Business Continuity Planning (BCP): On BCP at the bank, in order to figure out how IS/DFS systems can resume normal operations during a disaster, the business continuity officers are, as reported, works with each business unit at the bank as closely as possible.

Disaster Recovery (DR): the bank works with IT/IS subject matter experts (SMEs), to figure out a way to bypass for example a particular electronic feed or file dependency that may be needed to continue the recovery of a DFS system.

Backups at the bank are used for complete IS/DFS system restoration. Backups are also extended to saving more than just digital data. Backup processes include the backup of IS/DFS system specifications and configurations, policies and procedures, equipment, and data centers.

Security Organization: The bank maintains a fairly safe circle of IS/DFS security practices. These include; User Authentication-all employees within and without a bank uses one or a combination of the following; Something he/she knows (a password or PIN), Something he/she has (a card or token), Something he/she is (a unique physical characteristic).

Application Security: The bank employs both network and computer-based control of applications. Respondent #BOA09 had this to say: 'we do control applications on the network, by allowing or denying the network connections required for the applications to communicate.'

Computer Security: The bank is using best practices to secure both Windows and Unix systems alike as described by Respondent #BOA04: 'we are doing our best to reduce the attack surfaces, run security software and antiviruses, apply vendor security updates, perform strong authentication, and control administrator privileges. However, out of the box, Windows contains many vulnerabilities that leave it open to attack, but we are trying our best to reduce those vulnerabilities in a number of ways. Whether a server or a workstation, the approach is the same'.

Network Security: The bank uses a combination of security mechanisms to secure its network including using routers and switches to increase the security of the network, Virtual Private Networks (VPN), unified threat management platforms (firewalls combined with network antivirus, web filtering, IPsec, and other network-oriented security functions). The bank however does not perform application network communication control, advanced wireless network hardening practices and this is found to be a serious security concern.

Storage Security: One of the primary concern of network security is to protect assets that reside on the network and the most significant of those assets is data. The bank boast of a modern and complex Storage Area Network (SAN) with built in

security capabilities. Separation of duties is however found to be lacking within the storage infrastructure of the bank.

Database Security: Many of the security-related best practices have been deployed by the bank to secure database systems including network-level security, physical security, and using server-related best practices. However, there are additional considerations that should be taken into account when securing databases.

Physical Security: The bank carries out a number of measures to ensure the physical security of IS/DFS infrastructure including; classification of assets which is the process of identifying physical assets and assigning criticality and value to them in order to develop concise controls and procedures that protect them effectively, building access control systems, mantraps at the entrance, locks, bugler-proof doors and file cabinets, laptop locks and docking stations, controlled access to data centers, wiring closets, and network rooms, building and employee IDs, biometrics, security guards, physical intrusion detection (e.g. Closed-Circuit Television-CCTV, alarms).

The bank is integrating old legacy systems with modern solutions in an endeavor to modernize their systems. This however, has been a huge hassle for the bank in the process of seeking to improve DFS. One of the challenges is that some of the modern cloud and other SaaS solutions are incompatible with the older legacy systems. This means that in order for the systems administrator incorporate new tools and programs, extensive custom code is required to make it work. This has resulted to the emergence of data silos at the bank, whereby different departments across the bank cannot freely access the data they need.

Talent and Training: The bank employs a reasonable number of talented IS/IT employees with an average of 5-10 years of work experience. However, the IT/IS department at the bank is suffering from gaps in critical skills areas such as cybersecurity, cloud computing and DevOps.

Banking Industry Practitioners

Ugandan banks functions in a dynamic operating environment marked by rising customer expectations, a constantly changing economic landscape, widening scope and intensity of industry regulation. It is leveraging less of technological innovation geared towards IS/DFS systems risk management, while at the same time staying less vigilant against evolving IS/DFS systems risks.

For the last few decades, the global technology industry navigated talent supply challenges quite effectively. At the beginning, Ugandan banks attracted science, technology, and engineering talent from around the globe to work in its tech departments but this has since changed.

4.1.3. Summary

The respondents in the interviews raised valuable and important points both anticipated and expected through directly answering questions, and through presenting views in open and closed-ended questions and focused group discussions. The various categories obtained included issues directly addressing the concept of DFS delivery channels and models and DFS risks and risk management approaches.

The way most of the obtained views were inter-related suggests the richness of the topic of discussion, and acted as a pointer to possible future research in a qualitative method. The findings presented, interpreted, deliberated upon and theoretically contextualized in this chapter signify an attempt not only to reinforce ideas picked from the DFS and risk management literature but to unequivocally extend those ideas and bridge gaps in knowledge that would assist DFS providers, policy makers and practitioners in engaging in an innovative but yet risk aware DFS delivery.

4.2. Artifact Design

The framework design work was started by setting initial requirements which acted as guidelines for finding different theories in literature, especially about DFS and risk management. The findings from literature review were combined with practical/field experiences and study findings of the researcher and as a result of this combination, the Framework was designed.

4.2.1. Framework Structure

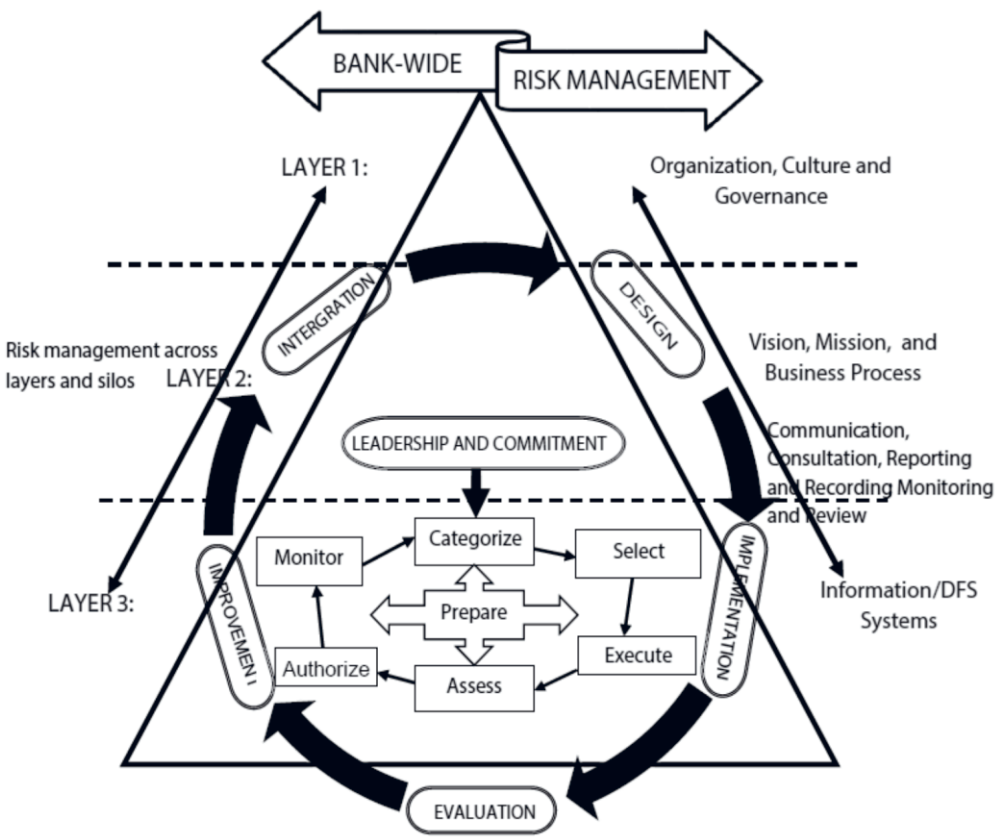

Figure 2: E-Risk Management Framework for DFS in banks

4.2.2. Framework components, process and contents

The framework adopts the ISO 31000:2018 framework design with a particular emphasis on Information/DFS Systems risk management incorporated with modification from NIST 2018 RMF. The framework works across three layers of the bank; Layer 1: Organization, culture, and governance, Layer 2: Vision, mission, and business process, and Layer 3: Information/DFS systems. The framework consists of six (6) major components: Leadership and commitment, Integration, Design, Implementation, Evaluation, and Improvement with seven (7) other steps (sub-components) focused on managing Information/DFS systems risk in banks; which are: Prepare (Process Initiation); Categorize; Select; Execute (Implement); Assess; Authorize; and Monitor.

4.2.2.1 DFS e-Risk Management Framework layers

Layer 1: Organization, Culture, and Governance: There should be adequate independence, accountability and segregation of duties involved in the oversight and management of DFS risks and the existing organization structure should allow for a bank-wide view of DFS risk management.

Layer 2: Vision, Mission, and Business process: Managing DFS risk in banks is a complex undertaking that requires the involvement of the entire bank. It should start from senior leaders providing the strategic vision and top-level goals and objectives for the bank, to mid-level leaders planning, executing, and managing DFS projects, to individuals developing, implementing, operating, and maintaining the Information/DFS systems supporting the bank's missions and business functions.

Layer 3: Information/DFS Systems: There should be a robust process in place to assess and monitor Information/DFS systems risk even at third party service providers. The questions to ask here include: 1) Is the Information/DFS Systems infrastructure appropriate given the DFS growth strategy and complexity of the DFS investments and type of DFS risks? 2) Are there adequate controls to guarantee DFS risk and finance data completeness, integrity and accuracy?

4.2.2.2 DFS e-Risk Management Framework components

- Leadership and commitment: Mandate and commitment from the Board is critically important and it needs to be continuous and high-profile. Unless this mandate and commitment are forthcoming, the DFS risk management initiative will be unsuccessful.
- Integration: This framework component includes; Determining management accountability and oversight roles and responsibilities; and Ensuring DFS risk management is part of, and not separate from, all aspects of the bank.
- Design: This component includes; Understanding the bank and its internal and external context; Articulating DFS risk management commitment and allocating resources; and Establishing communication and consultation arrangements.

- Implementation: This component includes; Developing an appropriate implementation plan including deadlines; Identifying where, when and how different types of decisions are made, and by whom; and Modifying the applicable decision-making processes where necessary.
- Evaluation: This component includes the following activities; Measuring the Framework performance against its purpose, implementation and behaviours; and Determining whether the Framework remains suitable to support achievement of objectives.
- Improvement: This component includes the following activities; Continually monitoring and adapting the Framework to address external and internal changes; Taking actions to improve the value of DFS risk management; and Improving the suitability, adequacy and effectiveness of the DFS RMF.

4.2.2.3 Information/DFS Systems risk management steps (sub-components)

The framework features the following steps (sub-components), incorporated from NIST 2018 RMF as part of the overall bank-wide risk framework—focused on Information/DFS Systems risk management:

- Prepare to execute the Information/DFS system RMF from an organization and a system-level perspective by establishing a context and priorities for managing security and privacy risk.
- Categorize the Information/DFS system and the information processed, stored, and transmitted by the Information/DFS system based on an analysis of the impact of loss.
- Select an initial set of controls for the Information/DFS system and tailor the controls as needed to reduce DFS risk to an acceptable level based on an assessment of DFS risk.
- Execute/Implement the controls and describe how the controls are employed within the Information/DFS system and its environment of operation.
- Assess the controls to determine if the controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying, for example, the security and privacy requirements.
- Authorize the Information/DFS system or common controls based on a determination that the DFS risk to bank operations and assets, individuals, and other organizations is acceptable.
- Monitor the Information/DFS system and the associated controls on an ongoing basis to include assessing control effectiveness, documenting changes to the Information/DFS system and environment of operation, conducting DFS risk assessments and impact analyses, and reporting the security and privacy posture of the Information/DFS system.

4.2.3. Framework Implementation Plan

To successfully implement the DFS e-Risk Management Framework, the initiative should be an on-going process on a continuous basis.

No.	Activity	Tools and Techniques
1. Planning—Implementing		
1.1	Identify intended benefits of the DFS RMF/initiative and gain board/executive level support	• DFS risk appetite • Corporate governance
1.2	Plan the scope of the DFS RMF/initiative and develop common language of DFS risk	• DFS RMF sophistication • Upside of DFS risk • Stakeholder expectations
1.3	Establish the DFS risk management strategy, roles, and responsibilities	• DFS risk management policy • DFS risk architecture • Level of risk maturity
2. Implementing—Measuring		
2.1	Adopt a suitable DFS risk assessment procedures and an agreed DFS risk classification system	• DFS risk protocols • DFS risk management guidelines • DFS risk classification systems • DFS risk description
2.2	Establish DFS risk significance benchmarks and undertake DFS risk assessments	• Benchmark tests of significance • DFS risk register
2.3	Determine DFS risk appetite and risk tolerance levels and evaluate the existing controls	• DFS risk appetite • DFS risk matrix • Loss control
3. Measuring—Learning		
3.1	Ensure cost-effectiveness of existing controls and introduce improvements	• DFS risk improvement plans • Reaction planning
3.2	Embed DFS risk-aware culture and align DFS risk management with other management tasks	• Control environment • Resource allocation • DFS risk communications • DFS Delivery/Business model

4. Learning—Planning		
4.1	Monitor and review DFS risk performance indicators (KPIs) to measure RMF contribution	• Audit plan • Sources of DFS risk assurance
4.2	Report DFS risk performance in line with legal and other obligations and monitor improvement	• DFS risk reporting

Table 3: DFS E-Risk Management Framework Implementation Plan

5. Conclusion

DFS have enormous potential to drive financial inclusion in low resource countries, but it's success will depend on having an appropriate risk management and regulatory framework that does not stifle innovation, as well as strong commitment, communication, support, and coordination from other partners and regulatory bodies. The rapid technology evolution comes with risks, and requires that Ugandan banks, partners and regulators stay in constant communication in order to assess the risks of each DFS product/service. The study identified a number of unmet requirement/gaps that demonstrate highly, the need for a DFS e-risk management framework in banks in particular and financial institutions in general.

Risk management in banks in this digital age is becoming more complicated than ever as security technology – including methods to evade it are gaining in sophistication. There is need for digital risk assessment to be put first by Ugandan banks and they should also reinforce an updated DFS risk management practices because this will ensure that all customer data is encrypted, private, and appropriately secured. As government and regulatory bodies are also becoming more aware of the risks of DFS and other digital operations at banks, regulations and compliance requirements must increase concurrently and banks should be held to a higher standard for maintaining security of DFS systems.

Banks in Uganda have not developed her own comprehensive DFS risk management reports and are relying on other related reports to monitor some risks that are directly linked to DFS. They also don't employ a comprehensive approach to DFS risk management, seldom integrating DFS risk management strategies in all areas of operations and in the organizational (bank) culture. There are also a number of unmet requirements/gaps in the way the security of DFS systems at the bank are managed. A set of framework design requirements/criteria were identified on the onset and two existing and commonly used RMFs (ISO and NIST) were reviewed and deemed applicable in designing a DFS RMF.

Finally, this framework addresses the needs of Ugandan banks. The banks may need to adopt and integrate all or parts of the framework. This framework should help to convince banks of the importance of institutionalized and integrated DFS risk management, but it is up to the bank to create the links between the various levels of operations and lines of authority. This study therefore furthers our knowledge of how DFS risk management can be implemented in banks.

6. Recommendations

The bank should consider the impact of change, innovation in technology and access to technology when providing: a) New DFS; b) Amending DFS; c) Curtailing DFS due to the adoption of technological solutions and efficiency driving measures, and; d) Training for employees administering DFS.

IT spend at this bank should be carefully balanced across three critical areas: customer expectations/services, cybersecurity and internal process.

The bank need to constantly refresh the talent pool. As made in numerous observations and studies, it is found that high-performing risk functions commonly depend on a high-performing IT and data infrastructure—for example, a central "data lake/repository" with harmonized definitions, architecture and clear data governance. There is unquestionable evidence that points that building the right mix of talent is equally important.

The bank should enhance and "reinforce" risk reporting especially for DFS risk. Better risk reporting is needed because of the ever-broader and cross-boundary regulation, and the need to adjust to market developments which require rapid, fact-based decision making. Paramount, is the recommendation for replacing paper-based reports with for example interactive tablet and mobile-based solutions that offer information in real time and enable users to do root-cause analyses. This would enable the bank to make better decisions faster, robustly and to identify potential risks more quickly as well.

In the process of managing short-term risks and priorities, risk management in the bank has to also focus on emerging risks which include; Industry disruption due to technologies, Availability of data, Industry disruption to new entrants, Integrity of data and data destruction, IT obsolescence, Model risk, Geopolitical risk, and Environmental risk or climate change. These risks may be "new kids on the block", previously less thought of or known but are increasing, and will definitely require more analysis, consideration and care.

The bank should build a strong risk-management culture. The activities of detection, assessment, and mitigation of DFS risk must become part and parcel of the daily activities of all the bank employees no matter the position and not only those in risk functions and senior management. With the continuous automation and more sophisticated and complex analytical and technical capabilities, human intervention is more than required to ensure appropriate and ethical application and deployment of risk management tools, technologies, policy and procedures.

DFS risk and risk management at this bank need to become a board-level concern. The Chief Risk Officer (CRO) need to establish ways of regularly monitoring DFS risks and providing an informed view to the bank and its management. In particular, the board at the bank need to be made aware of DFS risks and regularly updated on new developments and trends. DFS risk assessments should involve input from technology experts and other stakeholders across the bank; the bank need to set up a DFS working group that meets regularly. The CRO need to get closer to IT decision-making and establish strong links with their information security colleagues/department.

The bank need transformative new technology to address the ever-increasing complexity around managing risk and regulatory requirements. Some of the Important things the bank leaders must consider along the way are: preparing to implement changes without the need to complete a broad system rebuild, employing smarter software for risk management (Risk Monitoring and Management Information Systems—RMIS) and programs that are easily adaptable, and eliminating silos of data that currently exist between various systems in the financial environments. Advanced technologies such as big data analytics, service-based IT architectures, Artificial Intelligence (AI), and machine learning can help the bank harness the vast amounts of data at their fingertips to identify risks and opportunities with more precision, while responding more quickly to stakeholder demands. Risk management in these banks must keep pace with technology-driven change, and take the front seat in helping the bank to achieve digital ambitions.

The bank should regularly check its IT security. The ubiquity of digital technology in banking makes security a much bigger issue. With the constant and "break neck" speed of technology update/change in banks, the "ground-breaking" technology can become a liability if for example it leaks customer data or is hacked. The banks need to periodically and constantly review their security software and security policies. Fraud-detection and analytics technology has proven to be very helpful. It can help prevent intruders from breaching the bank's perimeter network and highlight and expose suspicious transactions at an early stage.

7. Suggestions for Future Research

The following suggestions for further/future research address contemporary trends in DFS risk management in the Ugandan banking industry and the insights gained herein.

One outstanding limitation is that this study focuses heavily on bank employees. It has not explored deeply other parties that may constrain and/or influence DFS risk management in banks. Future researchers could take into account other parties' interests; For example, the interests of the telecom industry, non-bank payment institutions, credit intermediation platforms, FinTechs, and BigTechs, etc. in the future of DFS risk management in banks.

Finally, further study is recommended into the expanding role of Ugandan banks as DFS providers in securing DFS and systems. This could for example include whether there are acceptable sensible limits to tasks given and what role a bank can play in enhancing cooperation in the security chain between other stakeholders in DFS risk management such as manufacturers of ICT/FinTech products, BigTech, Telecoms, and providers of ICT services and concurrently asking the "mammoth" question; does the current definition of a bank as a DFS provider match the reality of work asked and tasked?

Acknowledgement

Special thanks goes to our employers CANCOM Public GmbH, Berlin-Germany, Uganda Martyrs University, and our colleagues at the same organisations, most

especially Mr. Till Schwitalla and Mr. Georgi Pisin for their financial and moral support and patience.

Finally, this study would not have been possible without the help of colleagues in the case organization who accepted to be interviewed and provide the necessary information and documentation on DFS e-risk management in banks. These colleagues remain unnamed as stated in the informed consent, but they brought DFS e-risk management in banks – which is often an abstract concept – alive.

References

[1] Abrams, J., Carraro, M. & Ahmed, W., *Alternative Delivery Channels for Financial Inclusion: Opportunities and Challenges in African Banks and Microfinance Institutions*. The Master Card Foundation, Bankable Frontier Associates, 2016.

[2] AFI., *Digital Financial Services: Basic Terminology, Guideline Note No. 19*, Alliance for Financial Inclusion (AFI), 2016.

[3] AFI., *Uganda's Journey to Inclusive Finance through Digital Financial Services, Member Series: Financial Inclusion Journey,* Alliance for Financial Inclusion (AFI), 2019.

[4] C.C. Benson et al., *The Digital Financial Services Ecosystem,* International Telecommunication Union, 2016.

[5] R.A. Caralli et al., *Improving the Information Security Risk Assessment Process,* Carnegie Mellon University: Report Number: CMU/SEI-2007-TR-012, 2007.

[6] CSFI., *Finance for all: Wedded to FinTech, for better or worse,* Centre for the Study of Financial Innovation (CSFI), New York, 2018.

[7] CGAP., *Digital Financial Inclusion: Implications for Customers, Regulators, Supervisors, and Standard-Setting Bodies*, CGAP, 2015.

[8] P.L. Chatain et al., *Protecting Mobile Money against Financial Crimes: Global Policy Challenges and Solutions.* Washington DC: The World Bank, 2011.

[9] L. Denyes and S. Lonie*., Digital Financial Services and Risk Management*, ISBN: 975-0-620-71506-5. The Master Card Foundation, The World Bank Group, 2017.

[10] S. Frenkel, "Hackers Find 'Ideal Testing Ground' for Attacks: Developing Countries". The New York Times, July 02 2017. Available: https://www.nytimes.com/2017/07/02/technology/hackers-find-ideal-testing-ground-for-attacks-developing-countries.html.

[11] ISO, *ISO 31000 Risk management—Principles and guidelines*, International Organization for Standardization, 2018.

[12] C. Kasemiire, & D.V. Ajuna, "Hackers steal billions in mobile money heist", October 06 2020, Available: https://www.monitor.co.ug/uganda/news/national/hackers-steal-billions-in-mobile-money-heist-2458494

[13] J. Lamb, & S. Polverini, Assessing *risk in digital payments*, Bill and Melinda Gates Foundation, 2015.

[14] Morrow, R., Rodriguez, A., & King, N. (2015). Colaizzi's descriptive phenomenological method. *The Psychologist*, 28(8), 643-644.

[15] MicroSave, *Digital Financial Services Volume V: Optimising Performance and Efficiency Series*, MicroSave, 2015.

[16] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, Gaithersburg: National Institute of Standards and Technology, 2018.

[17] T. Nyirenda-Jere, & T. Biru, "Internet Development and Internet Governance in Africa". September 07 2018, Available: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Internet%20development%20and%20Internet%20governance%20in%20Africa.pdf.

[18] A. Osterwalder, Y. Pigneur, & A. Smith, *Business Model Generation.* Self-published, 2010.

[19] Responsible Finance Forum, *Opportunities and Risks in Digital Financial Services: Protecting Consumer Data and Privacy*. GPFI, GIZ, and IFC, 2017.

[20] T. Shaw, M. Willis, D. Skoog, S. Arenaza, S. Garg, S. Salerno, E. Hamilton, & S. Adnolfi, *Digital Financial Services Risk Assessment for Microfinance Institutions: A Pocket Guide*. The Digital Financial Services Working Group, 2014.

[21] Shiloh & Fassassi. "Cybercrime in Africa: Facts and figures". SciDev, November 20 2016, Available: https://www.scidev.net/sub-saharan africa/icts/feature/cybercrime-africa-facts-figures.html.

[22] The Gates Foundation, "Assessing Risks in Digital Payments", The Gates Foundation, August 26 2014, Available: www.gatesfoundation.org

[23] E. Tumusiime-Mutebile, *Remarks by Prof. Emmanuel Tumusiime-Mutebile, Governor, Bank of Uganda, Uganda Bankers' Association. Annual Bankers' Conference, July-19-2017*. Kampala: Bank of Uganda, 2017.

[24] E. Tumusiime-Mutebile, *Remarks by Prof. Emmanuel Tumusiime-Mutebile, Governor, Bank of Uganda at the Launch of Standard Chartered*

Bank (U) Limited's Client Digital initiative, January-29-2019. Kampala: Bank of Uganda, 2019.

[25] UNCDF, *Digital Financial Services in Uganda.* United Nations Capital Development Fund, 2014.

[26] UNCDF & European Investment Bank, *Digital Financial Services in Africa: Beyond the Kenyan Success Story.* United Nations Capital Development Fund, 2014.

[27] J. Wamema, *Developing Business/Information Technology Strategies*. Uganda Martyrs University-Kampala, 2018.

[28] K. Zeter, "That insane, $81M Bangladesh Bank Heist? Here's what we know". Wired, May 20 2016, Available: https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/

[29] C. Duden, "Five Steps of the Digital Risk Management Process". 360factors. Inc., August 08 2018, Available: https://www.360factors.com/blog/five-steps-of-risk-management-process/