ADDIS ABABA UNIVERSITY
COLLEGE OF BUSINESS AND ECONOMICS

Digital Financial Services and Operational Risks in Ethiopia: Implications for the Necessary Regulatory Frameworks

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF BUSINESS ADMINISTRATION

BY

MAHLET TSEGAYE

ADVISOR

Abebe Yitayew (PhD)

May 2024

ADDIS ABABA, ETHIOPIA

DECLARATION

Under my direction and counsel, I, the undersigned, thus declare that this thesis project, "Digital Financial Services and Operational Risks in Ethiopia: Implications for the Necessary Regulatory Frameworks," is my original work. Every source that I have cited or used has been properly referenced and noted.

Declared by: Mahlet Tsegaye Belete

Name: _____

Signature: _____

Date: June 6, 2024

Confirmed by Advisor:

Name: Abebe Yitayew

Signature: _____

Date: June 06, 2024

CERTIFICATION

This certifies that Mahlet Tsegaye has completed her research on the subject of "Digital Financial Services and Operational Risks in Ethiopia: Implications for the Required Regulatory Frameworks." This study is a unique piece of work that can be submitted to be awarded an MBA.

Advisor: _____

Addis Abeba University
College of Business & Economics

MBA Program

Digital Financial Services and Operational Risks in Ethiopia: Implications for the Necessary Regulatory Frameworks

By

MAHLET TSEGAYE

Approved by the Board of Examiners:

Bezbe T. Tayo
Advisor

Signature

Tenkir Seifu(PhD)
Examiner

6/28/2024
Signature

Abebaw Kassie
Examiner

Signature June 28, 2024

Contents

List of Tables

List of Figures

ACKNOWLEDGEMENTS

*” Those who complete the course will do so only because they do not, as fatigue sets in, convince themselves that the road ahead is still too long, the inclines too steep, the loneliness impossible to bear and the prize itself of doubtful value.” ~**Thabo Mbeki***

Without the support of God, I would not have progressed this far. Without my mother, I never would have begun and completed the task. My advisor Dr. Abebe Yitayew who helped me grow and add knowledge through the process of preparing this paper, always thankful. My spouse, who provided me with moral support. My strength came from carrying the support of my family and friends who offered advice along the journey. Thank you all and this is the fruit.

Abbreviations

PII	Payment Instrument Issuer
PSO	Payment Service Operator
NBE	National Bank of Ethiopia
GDPR	General Data Protection Regulation
AML	Anti Money Laundering
DFS	Digital Financial Service
USSD	Unstructured Supplementary Service Data

Abstract

Research aims: This research aims understanding the nature of operational risks as well as review of existing regulatory frameworks.

Design/Methodology/Approach: By using qualitative research methods, face to face as well as virtual interviews with fintech representatives (CEOs, risk management experts, legal personnel), and bank CTO (chief technical officers) the task was able to secure important information. The data was thematically coded and validated with the above data sources.

Research findings: Analysis revealed: (1) even officers at the respective organizations do not give many emphases to operational risks compared to the others, (2) there are new and innovative ways and approaches that fraudsters use to convince novice digital financial service users, (3) existing regulatory frameworks are not up to date, not complete enough to deal with such sophisticated approaches.

Research Recommendation: the researcher recommends the regulatory body to begin collaborating closely with the providers of digital financial services in order to establish regulations, develop close monitoring protocols, and develop a strategy for continuous improvement in closing the gaps and creating a suitable environment for the digital financial industry.

Key words: Fintech, digital financial services, operational risk, fraud

CHAPTER ONE: INTRODUCTION

1.1. Background

The exchange of money is growing commonplace. Businesses transact to sell/buy goods and services, individuals transact to purchase goods and services, and banks and/or non-bank financial entities transact to pay salaries. Ethiopia was once a very cash-based nation, but things are quickly changing now. The goal of the government is to make the nation a cashless society. The government has been working on initiatives lately to create Digital Ethiopia by 2025.

National Digital Payments Strategy 2021–2024 was published by the National Bank of Ethiopia which the government is highly supporting to bring a conducive regulatory environment to the fintech industry. The NBE has approved a number of important directives that would enhance the regulatory framework for low-cost distribution methods and permit new participants, such Fintech firms and telcos, to enter the financial services industry: (Ethiopia's National Digital Payments Strategy 2021-2024).

When we see where this move will take us as a country, dependence on technology will increase, including the financial ecosystem. Instead of dependence on traditional banks will move to fintech service providers (banks and non-banks). FinTech, which stands for financial technology, refers to financial advancements made possible by technology. Along the financial services value chain, all of the major players—from "start-ups" to "big techs" to established financial institutions—are utilizing this technology advantage to give customers experiences that are quick, easy, and unique. The aim has been to offer a payment system that integrates the features of increased convenience, safety, security, and accessibility while utilizing technology advancements that facilitate expedited processing. Other areas of emphasis have been protection, customer awareness, affordability, and interoperability (Shri Shaktikanta Das,2019).

Financial technology (Fintech) is a great breakthrough in changing the lives of societies. It made financial services accessible for societies across nations. The fintech industry is a

growing industry that financial service providers like banks and non-bank fintech companies are interested in starting to provide the service. Additionally, the legal environment has promoted this increased non-bank entity activity in the payment space. (Shri Shaktikanta Das,2019).

The emergence of new technologies has altered the way financial markets are operated, regulated, and overseen, posing new opportunities and problems to financial organizations, regulators, and consumers alike. (Gurrea-Martínez & Remolina, 2020). It is doubtful that the existing regulatory strategy will result in major structural change because it is subject to considerable political economy and coordination costs. FinTech can increase access to services and financial stability, but this calls for a major shift in the regulations' primary focus. (Philippon, 2017).

Sub-Saharan Africa has great potential for FinTech. A general pro-FinTech feeling is ensured by the possibility of financial inclusion and the lack of significant crises brought on by the new technology. As the pioneers in Sub-Saharan Africa for FinTech, Kenya and South Africa handle different difficulties as they arise and lack a comprehensive legal framework tailored to the sector. In the process, they frequently find it difficult to keep up with the rapid advancements in technology, but they also sometimes try to take proactive steps (such issuing cautions about the risks associated with using specific new technologies) (HeinOnline, 2024).

It is anticipated that these directives will have a major impact on the financial sector's expansion. To make sure the directives produce the desired results, the NBE will employ an incremental approach and closely monitor how the digital payment ecosystem implements them (Ethiopia's National Digital Payments Strategy 2021-2024).Because of the rapidly changing characteristics of the fintech environment, The risks associated with big tech operations in finance may not have been properly addressed by the current regulatory framework and are still a challenge (Crisanto, 2021). This demands a close examination of what works and what does not work.

Fintech is here for the betterment of the country. Businesses and customers have to be protected enough by regulating risk areas. One crucial step in encouraging credit institutions to place a higher priority on the management of operational risk-generating events has been the inclusion of operational risk in their capital requirements. In the Basel Committee's original plan (Basel Committee, 2011), with the exception of the portions related to credit or market risk, the operational risk was defined by the entire potential loss. The present methodology is more accurate and addresses the possibility of documenting direct or indirect financial losses due to (a) incorrect or insufficient internal procedures; (b) misbehaving individuals; (c) poorly executed systems; or (d) unfavorable external occurrences. Legal risk incorporates operational risk, while reputational and strategic risks are seen as separate entities. (Pepi, 2019). Operational risk is the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events (Bank Risk Management Guidelines (Revised),2010).

Every fintech and government wants a safe and sound digital environment, successful and accurate transactions, and a risk-free and error-free financial ecosystem. One operational risk that fintech companies encounter in their day-to-day operations is transaction mistake. Mistakes resulting from many causes during transactions can generate significant losses for people, fintech businesses, or the nation as a whole.

A study that aims to characterize the many types of mobile banking fraud and determine the amount of money lost or stolen in a year, from February 2022 to January 2023, and the resulting harm to society.” Characterizing Mobile Banking Transaction Fraudulent Activities” found of the 717 cases that were looked into, 162 or so cases involved financial losses as a result of fraud schemes informing the subscriber as if the person has won the lottery system organized by the Bank that the fraud victim uses. According to data gathered from the Federal Police and Commercial Bank of Ethiopia, there are approximately five additional types of fraud that have been identified. These are classified as "scammed technical," "robbed / lost mobile phone," "unknown phone number attached to bank account," "SIM card taken with fake ID / identity theft," and "fund transferred by a friend

or others." These categories account for 241, 278, 5, 20, and 11 cases, respectively, with a total loss of money exceeding 62.9 million Birr (Abel,2023).

In this regard, regulatory gaps also are not helping the service providers to emphasize frauds made because of people and processes. The condition in Ethiopia is indifferent to these problems. The National Bank of Ethiopia mentioned regulation as one of the challenges for digital payments in Ethiopia and mentioned the necessity of vigilant oversight to guarantee that the instructions are followed and result in the desired results (Ethiopia's National Digital Payments Strategy 2021-2024).

Transactions may fail from Internal Frauds (Theft by employees, knowingly reporting positions falsely, and insider trading using an employee's account), External Fraud (including counterfeiting and robbery), System and hardware failures, utility outages, and communication issues can cause business disruption. Execution, delivery, and process management issues include data input errors, collateral management lapses, unfinished legal paperwork, and vendor disagreements and other events (Table 1: Operational risk event types). This makes it possible for irresponsible people to steal money that is not theirs, harming both people and businesses in the process.

Research from around the world and continents demonstrates the need to manage operational risk. Studies conducted in the nation also demonstrate how minimizing operational risks has a good impact on performance. In this sense, the research will contribute to the corpus of knowledge already present in the academic setting and benefit fintech, regulators, and future researchers.

This study's goal is to ascertain the operational risks that are now present in Ethiopian Fintech services, to point out areas where the current regulation is deficient, and to recommend changes to the operational risk regulation.

The study's background will be covered in this chapter's introduction, which will also include a problem description, research questions, general and specific objectives, methodologies, study importance, study scope, and study constraints are all included.

1.2. Statement of the Problem

We tend to think of the possibility of these systems collapsing as something very unpleasant since we are part of structured societies that rely on the smooth operation of systems like the financial system, chemical plants, energy networks, air transportation, and nuclear facilities. Systems of law and regulation play a part in preventing such incidents. How to implement measures that will reduce the danger of damage from operational failure is a dilemma for legislators and regulators alike. The latter is based on the supposition that agents responsible for these issues act by commission (willfully) rather than by omission (as a result of mistaken action or erratic behavior), and that even in the latter case, the negligence that motivates their actions can be at least partially avoided if the agents are aware of the consequences. Legislators are frequently asked to set up circumstances that will, if at all possible, stop wrongdoings or conflicts from going to court. The interests of society are more important than enforcing penalties. Regulatory contracts, or agreements whose compliance is overseen by authorities, are thought to be the best course of action in many situations (Kyrtsis, 2009).

Operational risk management is much more than just a data collecting and risk identification technical procedure. In order to identify organizational categories of error, mistake, and anomaly and place them as risks for decision-making purposes, data collecting is a constitutive and performative activity. The behavioral difficulty of data gathering also extends to the organizational ability to leverage "new" data sets to question established cultures and practices, as well as the banking staff's "buy-in." An operational risk management conundrum may arise. On the one hand, the historical experience of low likelihood, big effect events—the rogue trader paradigm—dramatizes this emerging managerial and supervisory category. Conversely, internal agents' current risk management practices for medium-to-high probability and medium-to-low impact occurrences are

shaping the field of operational risk management. The operational risk agenda is defined by these agents, who include internal auditors and attorneys, in their own words (Power, 2005).

Organizations gather the information that these agents deem pertinent to operational procedures and develop operationalizable concepts of error, even if they might not line up with the requirements as first stated. Additionally, the requirement for quantitative modeling of operational risk and the established confidence in quantifying it are some of the factors driving these data collection initiatives (Power, 2005).

According to research on "The effect of risk management on financial performance: the case of commercial banks in Ethiopia," Ethiopian commercial banks should engage in appropriate credit, liquidity, operational, and market risk management to ensure the safety of their institutions and produce positive profits. This will help them to maintain a proper balance between risk management practices and financial performance. (YOHANNIS,2021).

Supervisors and the banking sector have come to understand the role that operational risk plays in determining the risk profiles of financial institutions in recent years. Operational risk exposures may be significant and increasing, as evidenced by developments like the use of more highly automated technology, the expansion of e-commerce, large-scale mergers and acquisitions that test the viability of newly integrated systems, the emergence of banks as very large-volume service providers, the increased prevalence of outsourcing, and the increased use of financing strategies that lower credit and market risk but increase operational risk (“Regulatory Treatment of Operational Risk,” 2001).

The Ministry of Justice said during a meeting that during the previous four years, scammers stole 1.8 billion birr from banks. What consumers lost as a result of mobile banking fraud is not included in this (Berhane, 2022). To showcase the extent of the damage below is a snapshot (Annex 1).

The lack of research databases in Ethiopia makes it necessary to conduct studies that highlight the need for regulations to manage operational risks. This will assist the regulator in understanding the necessary regulations and expediting their implementation, thereby improving the operating environment for fintech companies.

1.3. Research Questions

In this research, the below questions will be answered.

1. What are the prevailing operational risks in Fintech services in Ethiopia?
2. What are the gaps in the current operational risk management regulation?
3. What needs to be added/modified in operational risk management regulations?

1.4. General Objective

This study aims to identify the most important operational risks that require regulatory control and investigates the existing regulatory gaps and mitigation strategies for operational risk.

1.5. Specific Objectives

1. To identify the prevailing operational risks in Fintech services in Ethiopia.
2. To identify gaps in the current operational risk management regulation.
3. To suggest areas of operational risk management regulations.

1.6. Significance of the Study

Fintech companies adhere to bank-led regulations, which may vary from their operational conduct. A better suited environment will be introduced to the fintech environment and the financial industry at large if regulations are based on the nature of the fintech industry. The study's findings will be beneficial.

- ✓ Added knowledge on which regulatory aspects to prioritize for policymakers.
- ✓ For Fintech companies to review the current operating way of handling operational risks.
- ✓ End users to understand the operational risk and protect themselves.
- ✓ Serving as a catalyst for more research.

1.7. Scope and Limitation of the Study

1.7.1 Scope

The purpose of this study is to use a qualitative research approach to identify the top operational risks that require attention from the regulatory body and to investigate the gaps and remedies that exist in the current regulations related to operational risk mitigation. The below cases can be mentioned as a challenge in operating in the environment

- Integrations issues – deducting from customers but the services are not delivered (mobile card recharge)
- Manual operations in between platforms – (inputting the figure wrongly, or repetitive addition of an amount)
- Transferring to wrong accounts
- Forced theft – being pushed to transfer to the theft account through mobile
- Fraudsters impersonating customers
- Social engineering – collaborative did by staffs and outsiders and embezzling customers
- Commission arbitrage by agents – finding gaps and using that
- Data loss – having no data recovery point, redundancy including Geo redundancy
- Overdraft
- Not closing accounts of agents intime when their contract ends
- Outdated platforms

The data from fintech service providers (private fintechs and banks that started digital financial services) will be gathered using semi-structured interview questions for the reason that the gaps and challenges are being faced and handled on a day-to-day basis.

1.7.2 Limitation

This study is restricted to the operational hazards associated with fintech transactions in Ethiopia.

1.8. Organization of the Paper

The background, Statement of the Problem, research questions, general and specific objectives, significance, scope, limitations, and organization of the paper are all included in Chapter One, the introduction.

Chapter Two Covers Theoretical Review, Review of Empirical studies, operational risks in FinTech, Regulatory needs related to operational risks, Current fintech landscape, Ethiopian context, and research gaps.

Chapter Three discusses research design, sample design, data collection, data analysis, a nd ethical considerations.

Chapter Four presents the findings, and discussion.

Chapter Five provides a summary, conclusion, recommendation, limitation, and future r esearch.

CHAPTER TWO: Literature Review

This chapter summarized and reviewed a number of articles.Gaps in past research will be identified and the contribution this study will make to filling those gaps will be discussed.

2.1 Theoretical Review

Definition of operational risk

Operational risk is defined as "The risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events" is the definition of operational risk. Due to significant losses incurred due to operational risk, a number of globally operating banking institutions have been allocating internal economic capital for operational risk for a while now. Given the variety of risk management strategies employed by banks, the operational risk proposal's flexibility makes sense. However, consistent supervisory implementation is challenged by this flexibility. Since banks are concentrating on internally consistent models, uniform supervisory treatment from various industry viewpoints is necessary. One issue supervisors face is the uneven categorization of operational losses, which makes comparisons between institutions and industry-wide studies more difficult. Internal operational loss data from banks is gathered in accordance with guidelines established by risk managers who oversee the entire company. Nonetheless, it can be challenging to classify loss data, and reasonable people may categorize the same occurrence under multiple business categories or event kinds (Barriga & Rosengren, 2006).

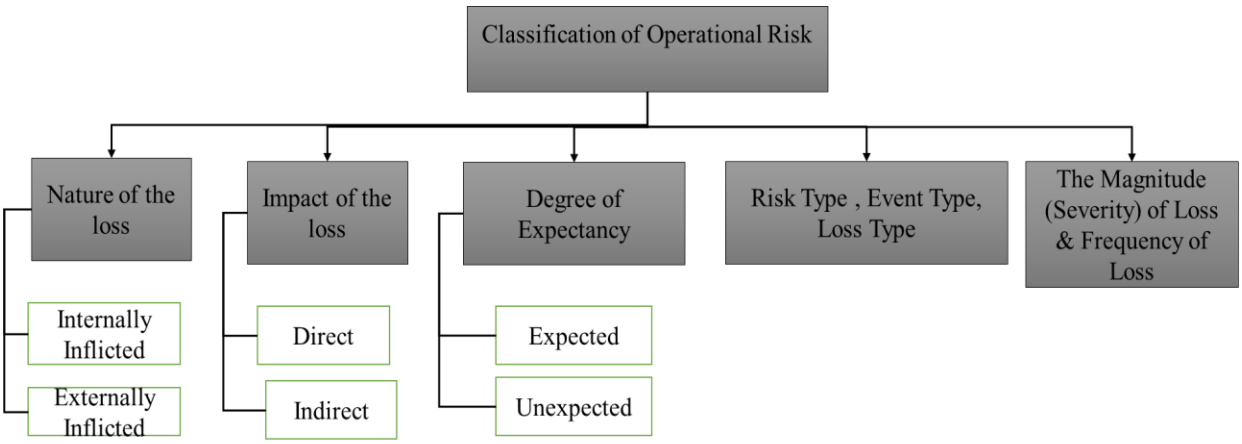


Figure 1:Operational Risk Classification (Izhar, 2012).

Internally inflicted The majority of losses resulting from process, technological, and human faults, including those brought on by internal fraud, injuries, unauthorized trade, computer malfunctions, and telecommunication issues, are considered internal sources of damage. Man-made events like outside fraud, theft, computer hacking, terrorist attacks, and natural catastrophes like storms, floods, and fires that cause physical asset destruction are examples of external sources.

External sources comprise both natural and man-made events, such as physical asset damage from storms, floods, and fires, and man-made catastrophes like external fraud, theft, computer hacking, and terrorist actions.

Direct losses are the losses that result immediately from the related incidents. Generally speaking, indirect losses are opportunity costs and the losses incurred in resolving an operational risk issue, including near-miss incidents (Izhar, 2012).

The anticipated losses are typically those that happen frequently, like every day, like small-scale credit card fraud and personnel errors. To put it another way, **expected loss** is predicted for the upcoming time frame. Conversely, **unexpected losses** are those that are typically difficult to predict, like massive internal fraud and natural disasters (Izhar, 2012).

Based on the fourth category Operational risk can be classified as below (Izhar, 2012)

Hazard constitutes one or more factors that increase the probability of occurrence of an event.

An event is a single incident that leads directly to one or more effects (e.g. losses).

Loss constitutes the amount of financial damage resulting from an event

Operational losses can be also broadly divided into four primary categories based on **Frequency/Severity** (Izhar, 2012):

(i) Low frequency/low severity

(ii) High frequency/low severity

(iii) High frequency/high severity

(iv) Low frequency/high severity

Both high frequency/high severity and low frequency/low severity are impractical. Losses with a high frequency but low severity are usually avoidable and of little consequence to an organization. The losses with low frequency and high severity are what inflict the most damage. Banks need to pay extra attention to these losses because they have the most financial ramifications for the organization, sometimes leading to bankruptcy. A small number of these occurrences could lead to bankruptcies or sharp drops in the bank's value. (Izhar, 2012).

Monetary Transaction

Any transaction involving one institutional unit making a payment, receiving a payment, incurring a liability, or receiving an asset that is expressed in units of currency is considered monetary (“System of National Accounts,” n.d.).

Difficulties in Risk Modelling

The most evident problem is that market risk and credit risk have comparable characteristics. Both of them are defined by the idea of "risk exposure," and they are both rated and assessed according to industry-wide criteria for the likelihood of a loss event.

These characteristics are absent from operational risk, mostly due to the lack of an organized, reliable, industry-accepted procedure for gathering and compiling the data (Sherwood, 2018).

Hidden Operational Risks

Operational risks are inherent to operational processes, even though they can have external causes or be connected to the breakdown of systems and human resources that help to carry out corporate operations. Therefore, there are two primary and easily identifiable types of hidden operational risk: unanticipated external events (of a kind not previously encountered or understood) and events that are so intricately woven into the supporting process resources that they are challenging to recognize and track. Unless there are significant advancements in the field of clairvoyance, the first category will always provide challenges; however, the second category is more under our control. The hazards inherent in the documentation supporting business processes are arguably the most glaring example of this second group, and contracts have to be one of the most concerning document types among them (Sherwood, 2018).

Data Collection Issues

Regarding market and credit risk, all information is readily available in an electronic format. Because automated systems can gather, compile, and evaluate this data, historical loss records are comprehensive, uniform, and homogeneous. In terms of operational risk, things couldn't be any different. Every loss event is the consequence of a complicated interaction between numerous possible causative elements, and a major loss event can typically be retroactively examined to determine the "unlucky" alignment of numerous minor factors, each of which would be regarded as inconsequential on its own (Sherwood, 2018).

2.2 Review of Empirical Studies

Nsaibi, Abidi, and Rajhi conducted a study titled "Corporate Governance and Operational Risk Empirical" to examine how governance structures impact banks' operational risk

management. According to the research, regulatory authorities are now primarily concerned with considering the relationship between banking governance and operational risk, particularly in light of the recent US crisis, which turned out to be a crisis of banking failures rather than the traditional crisis of insolvency risk. After reviewing the banking literature, we discover that there is never a consensus in the theoretical or empirical debate regarding the impact of internal mechanisms on the handling of operational incidents. As a result, the analysis of this impact is never conclusive because the findings of empirical studies are contentious. Because operational errors in the banking industry and financial system continue to occur, this discussion is still ongoing and relevant to risk managers, regulators, and scholars.

2.3 Operational risks in Fintech

Operational risk is generally understood to mean "the risk that the reduction, deterioration, or breakdown of services will result from human error, management failures, or deficiencies in information systems or internal processes." During business operations, a variety of operational risks may arise. Many fintech companies that are not banks concentrate more on cutting-edge technologies that boost speed. In order to maintain stability, lower fraud, manage data, and comply with regulations, businesses must modify their procedures. However, some businesses, particularly smaller businesses, have not lived up to these expectations. The primary obstacle faced by several fintech enterprises is adjusting to the frequently swift pace of industry transformation. (Kwon, Lee, & Owens, 2023).

The study "THE EFFECT OF OPERATIONAL RISK MANAGEMENT PRACTICES ON THE FINANCIAL PERFORMANCE IN COMMERCIAL BANKS IN TANZANIA" found that, of all the risks that occurred in commercial banks, operational risk accounted for 44%. This is because of the increased use of automated technology, the dearth of qualified personnel and management support within the institutions, as well as internal and external frauds (Meshack & Mwaura, 2016).

A different study cites several notable instances of operational risk events, such as the collapse of Barings Bank in 1995, the loss of 850 million euros at AIB in 2002 as a result of unauthorized trading, the unbelievable Bernard Madoff Ponzi scheme uncovered in 2008, and, most recently, the September 2011 loss of UBS as a result of rogue trading that exceeded 1.5 billion euros. Despite the fact that these incidents raised awareness of operational risk and its significance, operational losses continue to occur, and financial crises expose fresh shortcomings in the operational risk management procedures that are in place. Financial services companies' exposure to operational risk is evolving due to their increased reliance on automation and information technology, as well as the complexity of new products (Sturm, 2013).

The study is regarded as one of the rare studies that contributes to the analysis of the risks of adopting FinTech in banks and its impact on performance. It was found that cyber risks and operational risks of adopting FinTech hurt banks' performance. A bank will be exposed to operational risk when introducing fintech. Furthermore, it provides a clear image for bank decision-makers to recognize the negative aspects of FinTech adoption (Alshari& Lokhande, 2023).

Table 1:Operational risk event types

Loss Event Types and Examples	
Event Type	**Examples**
Internal fraud	Insider trading on an employee's account, deliberate misreporting of positions, and employee theft
External fraud	Stealing, counterfeiting, and check kiting
Employment practices and workplace safety	General liability, infringement of employee health and safety regulations, and workers' compensation and discrimination claims
Clients, products, and business practices	Violation of fiduciary duty, improper use of private client data, money laundering, and unapproved product sales
Damage to physical assets	Vandalism, earthquakes, fires, floods, and terrorism

Business disruption and system failures	Utility outages, telecommunication issues, and hardware and software malfunctions
Execution, delivery, and process management	Errors in data entry, inadequate collateral management, insufficient legal documentation, and disagreements with vendors

Source: ("FDIC: Federal Deposit Insurance Corporation," n.d.)

In response, institutions committed large sums of money to operational-risk capabilities. They created elaborate controls and control-testing procedures, established new risk-identification and risk-assessment methods, and generated risk taxonomies that went beyond the BCBS categories. Even though industry-wide regulatory fines were successfully decreased, operational risk losses have continued to be high (Figure 2). Following the 2008–2009 financial crisis, operational risk losses rose sharply and have stayed high ever since (Eceiza et al., 2020).

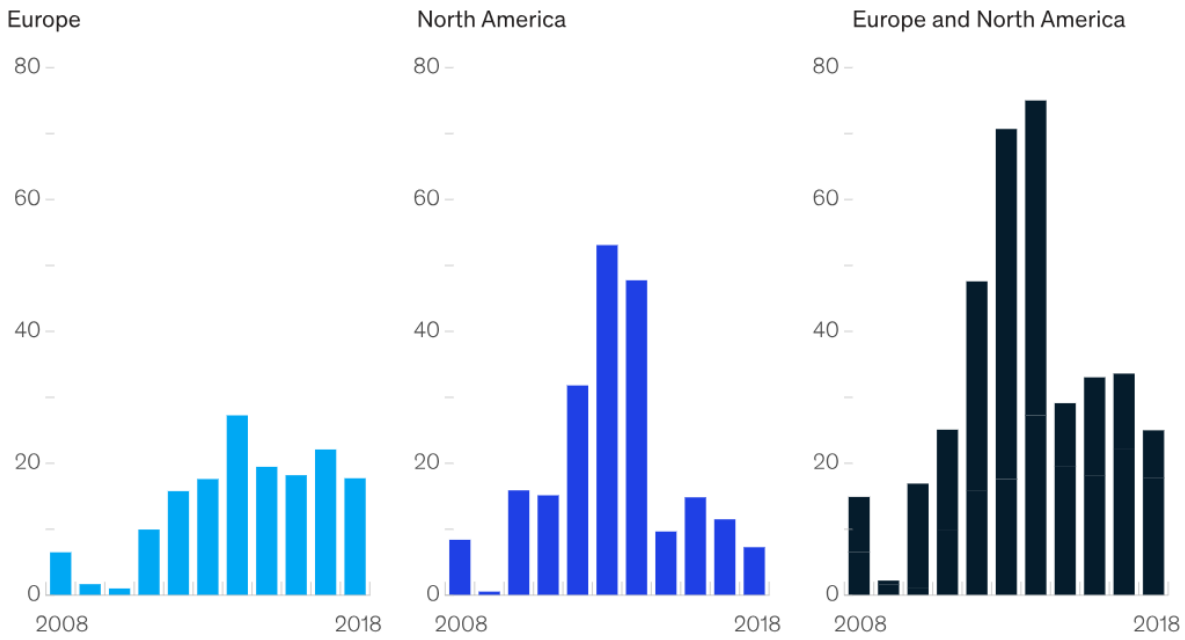


Figure 2: Banking litigation: costs, fines, and operational losses, $ billion

Source: (Eceiza et al., 2020)

When it comes to Ethiopia's position in tackling operational risk in the financial industry it shows a lot has to be done. As it is mentioned in publication Ethiopian commercial banks

adhere to a modified Basel I framework. Commercial banks are now required to calculate capital adequacy ratios using a modified form of Basel I, although the NBE intends to eventually implement Basel II (International Monetary Fund. Statistics Dept., 2020b). In other words, banks and non-bank fintech companies cannot follow any legal framework for operational risk management.

2.4 Regulatory needs related to operational risks

FinTech has drawn interest from investors and regulatory agencies worldwide due to its innovative offerings in banking and financial services goods and services. Fintech, which primarily aims to increase financial inclusion for the unbanked population in emerging economies through mobile devices, has emerged as a new commercial entity that promises to fulfill the World Bank's and G20 countries' millennium goals. Due to the widespread usage of mobile devices, FinTech companies have access to vast amounts of user data. These solutions, which are exclusive to each Fintech company, are continually evolving and drive sales of financial goods. Fintech has developed a business model to offer financial services such as digital wallets, digital currencies, crowdsourcing, wealth management, payment services, and FX services for remittance. Customers are connected through mobile phones and other financial services by a data-driven business model, which necessitates a new regulatory framework that safeguards consumers and keeps the economy from experiencing systemic risk. (Mahalle, Yong, & Tao, 2021).

According to the results of another study on "Combatting Operational Risk through Regulatory Technology," financial innovation has been welcomed by the local financial industry. It is clear that there is a desire to improve internal process efficiency and make it easier for adherence to new regulations, as institutions have acknowledged improving internal operations in an effort to increase digitization. Therefore, the regulator needs to stay up to date on the operational risks that come with using newer technologies and look at the tools that RegTech offers to help reduce these risks. In addition, the regulator must to promote innovation and technological advancement while maintaining the stability of

the financial system. The timing of new regulations must be carefully considered to avoid prematurely stifling growth (Ganpat & Harrypersad, 2018).

Financial regulators supply banks with a plethora of updated guidelines and regulations. To guarantee a bank's solvency, a specific set of guidelines specifies how much loss-absorbing regulatory capital must be calculated and placed aside (Aroda, 2016).

2.5 Current Landscape of Fintech

Following the Banking activity Amendment Proclamation's enactment in 2019, digital financial service providers have gained legitimacy as financial organizations capable of doing banking activity. The 2019 Banking Business Amendment Proclamation represented a significant change in that it permitted non-bank/non-microfinance entities (like technology companies) to participate in the banking business sector, subject to meeting the conditions outlined by the National Bank of Ethiopia. This is despite the fact that the proclamation did not permit foreign investment in digital financial service companies (Solutions,n.d.).

Ethiopia's financial services industry is still off-limits to international investment. In the larger financial services ecosystem, the involvement of a few foreign investors like M-Birr and Moneta (Amole) has been restricted to offering technology services (such as software platform provision and related technical help) to financial institutions that have been granted licenses (Solutions, n.d.).

Government officials' recent policy declarations suggest that the financial services industry is moving toward more accessibility for foreign investors and banks. Furthermore, the newly adopted National Digital Payment Strategy 2021–2024 anticipates that foreign fin-tech companies may play a role in the strategy's execution and participate in it (Solutions, n.d.).

The National Digital Payment Strategy (2021-2024) defines fintech as an organization regulated by a central bank to offer payment services and that leverages innovation in financial services enabled by technology (Ethiopia's National Digital Payments Strategy 2021-2024).

The new law exempts licensed telecom operators from the regulatory trend that up until now required financial institutions, such as Payment Instrument Issuers and Payment System Operators, to be set up as Share Companies with a minimum number of shareholders and a cap on shareholding. With the new law, licensed telecom providers in Ethiopia would not have to worry about shareholding cap restrictions when establishing a wholly owned subsidiary to provide digital financial services. The subsidiary might take the form of a Share Company or Private Limited Company (Solutions, n.d.).

About 22% of individuals in 2014 had accounts with official financial institutions, according to data from the Global Findex Database (Demirgüç-Kunt et al. 2018).In 2017, this figure rose to 35%, a 13 percentage point increase in just three years (Ethiopia's National Digital Payments Strategy 2021-2024).

All these developments in the country are helping to create a safe environment in digital financial services for those who are in the business already like banks, fintech, and telecom companies, and attracting new entrants.

2.6 Ethiopian context

With the launch of HelloCash and M-Birr, two mobile money providers, mobile banking was made available in 2015. Two years later, the CBE introduced its digital money transfer platform (CBE-Birr), and Dashen Bank's Amole mobile wallet followed suit. Two years ago, Awash Bank launched its "Awash Birr" platform (Fortune, n.d.).

These days, practically every commercial bank and microfinance institution (MFI) offers mobile money services. There are currently over a dozen active mobile wallet, money, and

banking platforms. Together, they made last year's trades worth 320 billion Br possible (Fortune, n.d.).

There are around 3.5 million users of Amole Wallet. With 5.4 million users on its platform, the CBE represents almost 40% of the nation's 14.5 million mobile banking consumers (Fortune, n.d.).

Industry participants believe that the main enabling elements are inadequate documentation, a lack of division of roles, and weak internal control (Fortune, n.d.).

With several parties sharing mobile money and other e-payment platforms, the risk becomes more apparent as the web gets more twisted. With the entry of financial tech (fintech) companies, the landscape of digital banking is evolving (Fortune, n.d.).

Only financial companies, especially banks and microfinance organizations, were allowed to offer mobile banking services until two years ago. This was altered in August 2020 when the central bank issued a directive enabling non-financial institutions to participate in the fray. The introduction of "Telebirr" by state-owned Ethiopian telecom last year changed everything (Fortune, n.d.).

Telebirr, one of the five non-financial companies with central bank permits, enables users to make deposits, withdrawals, and transfers of money via a USSD code or a mobile application. It has around 22 million members as of right now, outpacing most of its rivals in less than a year. It has made trades worth around 30 billion Br possible. But not without worries and dangers to one's security (Fortune, n.d.).

Recently, money transactions to Telebirr accounts registered in the name of another account user were suspended by Ethio Telecom. Additionally, bank-to-bank transfers have been restricted by central bank regulators, with a 25,000 Br transaction limitation (Fortune, n.d.).

2.7 Research Gaps

Even when studies on financial risks—more especially, operational risks—are conducted, they usually focus on the ways in which they improve organizational performance. Fewer studies have been conducted on the requirement for regulation-based control than localized management. Regarding banks and non-bank fintech service providers, no paper has been done in Ethiopia in this regard.

CHAPTER THREE: Research Design and Methodology

3.1 Study Design

This study aims to explore the operational risks that are now present, regulatory loopholes, and regulatory actions that can be taken to protect the fintech ecosystem. The qualitative aspect of this exploratory study makes it easier to get feedback on the urgent operational issues that fintech companies face locally. Since a fintech ecosystem is not an isolated one and a chain is only as strong as its weakest link, a regulating body is necessary. In a sense, the effectiveness of a single fintech in managing operational risk is not adequate as the whole eco system has to be in a similar level.

3.2 Sample Design

A defined strategy for selecting a sample from a specific population is known as a sample design. It speaks of the method or approach the researcher would use to choose the objects for the sample. The sample size, or the number of objects to be included in the sample, may also be determined by the sample design. Data collection precedes the determination of sample design (Kothari, 2004).

Purposive sampling will be used to choose samples based on the leaders' beneficial contributions.Put differently, purposive sampling involves the "on purpose" selection of units. This sampling technique, also known as judgmental sampling, depends on the researcher's judgment to determine which people, situations, or events will yield the most information to meet the goals of the study (Nikolopoulou, 2023)

In this study, purposive sampling is employed by focusing on senior management and staff members holding CEO roles, as well as those working in the operational, legal, and risk divisions of fintech organizations that are in close proximity to the research topic. The interview will be semi-structured in order to allow the interviewer to inquire further in light

of the respondents' responses and to allow for unrestricted data collecting that might reveal previously unreported viewpoints.

3.3 Data Collection

One qualitative research approach that uses questioning to get data is the interview. Two or more people participate in interviews, one of them being the interviewer who is asking the questions (George, 2023).

Differentiating between different types of interviews is generally based on how structured they are. Predetermined questions are asked in a predetermined order during structured interviews. Interviews that aren't planned are more conversational. Semi-structured interviews occupy a middle ground (George, 2023).

For this research a semi structured interview will be done by giving a room for more discussion from the responses the interviewee will provide. The interview will have questions in an open ended way.

3.4 Data Analysis

Since this research aims to get the views and perspectives on fintech operational risks and the support that can be given on the regulation aspect from the regulatory party both from fintech experts and the regulatory side, the thematic analysis will help to benefit from the research.

Although there are many different kinds of theme analysis, there are six general steps in the process. The process of doing a thematic analysis includes preliminary analysis, data classification, topic identification, and reporting (Thematic Research in Qualitative Research - QualTricS, 2023).

Familiarization – The research teams or investigators familiarize themselves with the dataset during the initial phase of thematic analysis. This could entail going over the material over and again and possibly transcribing it. Prior to assigning first codes, researchers may jot down their early ideas regarding any potential patterns they see in the data (Thematic Research in Qualitative Research - QualTricS, 2023).

Coding – Researchers can quickly and readily identify the ideas and topics in their data by using codes in thematic analysis. Text data snippets, as well as audio and video clips, can have codes assigned to them. This can be done in a more intuitive way or using a methodical and thorough approach, depending on the kind of thematic analysis that is being employed (Thematic Research in Qualitative Research - QualTricS, 2023).

Identifying theme – The broad concepts and topic areas included in the corpus of study data are known as themes. By compiling the findings of the coding process, researchers might find themes. These themes unite the detected codes into groups based on their meaning or topic matter (Thematic Research in Qualitative Research - QualTricS, 2023).

Reviewing themes – After defining the themes, the researchers revisit the coded data extracts to assess the themes' coherence. At this point, they might begin to arrange the topics into a conceptual framework or map (Thematic Research in Qualitative Research - QualTricS, 2023).

Defining and naming themes – Researchers start to give the themes names and more detailed definitions as they spend more time going over them. Themes differ from codes in that they are directly related to the study question and identify patterns in the data rather than just topics (Thematic Research in Qualitative Research - QualTricS, 2023).

Writing up – At this point, the researchers start working on the final report, which provides a thorough synopsis of the codes and themes along with excerpts from the original data that highlight the conclusions and any additional information pertinent to the investigation.

A review of the literature that cites other earlier studies and the findings that shaped the study topic may be included in the final report. Additionally, it can highlight areas that have emerged during the research process and that the themes support for further investigation (Thematic Research in Qualitative Research - QualTricS, 2023).

3.5 Ethical Considerations

Participants in the interview are asked for their permission to record the conversation and utilize all of the interview material for the purposes of this study.

CHAPTER FOUR: Analysis and Discussions

4.1 Introduction

The objective of this research is to assess the current operational hazards. The research findings are summarized and discussed in this chapter.

4.2 Finding

The below are themes for the research.

- ❑ Understanding of operational risk among fintech
- ❑ National Bank's Engagement level with fintech
- ❑ Operational risk Origins (Internal vs External risks)
- ❑ Operational Risks and Impact Assessment
- ❑ Operational Risk Participants
- ❑ Awareness and degree of knowledge
- ❑ Fintech Vs. banks' acceptance of current regulations
- ❑ What does the regulation have?
- ❑ Recommended Industry Best Practice
- ❑ Recommended focus areas for the regulatory

4.2.1 Theme 1: Understanding of operational risk among fintech

Almost all the respondent agree the understanding of operational risk is vague in the digital financial environment

"I can say it is not well defined and if defined also not implemented well."

"National Bank ask risk profile as one of monitoring aspect and since for the bank risk is as its DNA. There is risk due diligence and one of them is operational risk and we can question the maturity risk and the other thing IT risk as one of the operational risks is not available in strong way when organizing it in the risk department."

4.2.2 Theme 2: Operational risk Origins (Internal vs External risks)

All participants agreed that the operational risks that are raised from bank side(traditional fintech) is more but they focus on internal risks which they are in control of.

"When I start from external System rules are below standards in this market (security on the systems are below standards (outdates, very vulnerable,) people knowledge specially in the banking sector and the biggest also process (no outlines process from a regulatory side) and the regulator is new for this and that is a risk for the players"

"They happen mostly on Fintech operators which can be traditional fintech companies, banks or even telcos with mobile money operating licenses"

"I believe unlike other nations, our operational risk, particularly with regard to fraud, originates domestically because the national currency is the birr".

4.2.3 Theme 3: National Bank's Engagement level with fintech

All interview participants believe that the engagement level of National Bank of Ethiopia is very low compared to its engagement level with banks and they expect that will improve.

"Fully supported as the regulators will come up with laws that will create level playing field for all DFS operators, provide penalties for violations and also safeguard customers & partners."

"There is lack of sensitization and forums and harmonize guidelines ammonization has to be there from the regulator to have comment understanding and practice. You can be as good as your internal system, but partners weakness will affect you. Risk in digital payment affects all. Forums has to be there to learn and to share best practices. Need to review, put standard compliance and give certification."

"Payment of government services – this should be availed to all valid DFS operators."

4.2.4 Theme 4: Operational Risks and Impact Assessment

A formalized minimum impact level assessment for operational risk is not on the ground which all the interviewee mentioned and suggested that must be exercised.

"I expect the regulatory to come up with evaluating the number of customers impacted/defined timeline and how much by putting threshold."

"There was an incident that one of the partners that order a different number which the customer did not order from the bank to DFS side it goes to the wrong account and the bank did not want to take accountability because of reputational damage we took the loss."

4.2.5 Theme 5: Awareness and degree of knowledge

The interviewee mentioned also that the awareness level on the environment has big gap .

"When I start from external System rules are below standards in this market (security on the systems are below standards (outdates, very vulnerable,) people knowledge specially in the banking sector and the biggest also process (no outlines process from a regulatory side) and the regulator is new for this and that is a risk for the players"

"Third party risk is high which cannot be only risking that company, it touches across. So, from customers we see high volume of operational risk by wrongly sharing their information, but we try our best to give awareness."

"... we can question the maturity risk and the other thing IT risk as one of the operational risk is not available in strong way when organizing it in the risk department. It is in recent time in the bank also IT risk as a wing under operational risk. In relation to that from National Bank side under operational risk the technology related risks follow-up, KPI is lacking because of maturity and knowledge gap."

4.2.6 Theme 6: What does the regulation have?

The interviewee mentioned PSO and QR code standardization are there in the regulation.

"Proclamation for PSO is revised which addresses a lot of gaps including opening the business to foreign investors. Licensing and authorization of payment system operators and payment instrument issuers.

QR payment standard

Person to Merchant rule will come very soon."

4.2.7 Theme 7: Recommended Industry Best Practice

It was also mentioned for National Bank of Ethiopia to follow industry standards.

"i. Platform availability – this is brought about by downtimes which make platforms less reliable, this is addressed by proactive monitoring to pick incidents before they impact customers and also deploying platforms with high availability for disaster recovery.

ii. Fraud – malicious customers, agents & merchant take advantage of loopholes in platforms, processes to execute fictious transactions in order to gain financial benefit – this is mitigated by having proper fraud controls within the ecosystem to identify such behavior and take corrective actions/measures

iii. Money Laundering –proceeds from criminal activity which are introduced into mobile money ecosystem in order to appear genuine – this is mitigated by integrating the mobile money system to proper AML platforms which can pick out such transactions and flag them"

4.2.8 Theme 8: Recommended focus areas for the regulatory

In addition to what is there a number of recommendations were put by most of the participants of the interview.

"On process when there is incident in terms of communicating has to be there post incident and learnings."

"The regulatory should reinforce alert has to be there for systems, If transaction are going out of the normal trend also, decision makers has to be there, processes of approval at crisis has to be there, Documentation and lesson learned has to be there"

"There is a gap in the current regulation for us to know our responsibility. They think we are small and there is no platform that helps us to feedback. Who is measuring compliance is not clear."

4.3 Discussion

This study reassures us that the most damage is caused by low frequency/high severity losses. Because these losses have the largest financial ramifications for the institution—including the possibility of bankruptcy—banks need to pay extra attention to them. A small number of these occurrences could lead to bankruptcies or sharp drops in the bank's value (Izhar, 2012).

4.3.1 Understanding of operational risk among fintech

Even though fintech companies must submit a risk management framework in order to be licensed as issuers of payment instruments, they nevertheless face difficulties because of their weak operational risk management and occasionally absentee departments. Depending on the context, the operational risk management maturity level varies and poses challenges that the fintech must either work out a partnership with or decide not to incorporate. The lack of a dedicated and accountable division and the disregard for IT operational risks are further problems. The management of operational hazards is left to the discretion of individual companies due to its high level and lack of definition. Fintech companies find it challenging to work together because of this increased risk and exposure.

There are insufficient forums, unified guidelines, and sensitization. Regulations must be harmonized in order for comments to be utilized and understood. One respondent stated that partners' flaws can still hurt an individual even if they are as effective as an internal system. Everyone is affected by the risk of digital payments. Forums are vital for learning and sharing best practices. Certification, standard conformity, and review are necessary.

4.3.2 National Bank’s Engagement level with fintech

The regulatory function is important and indispensable. In contrast to banks, fintech companies believe that additional regulatory action is necessary.

Regarding the framework's setup, it lacks transparency, flexibility, and effectiveness. The regulatory framework is intended to be engaging. It is imperative that industry participants

arrive and design with a shared and lucid comprehension of essential frameworks. The players must put it to the test. As things stand, it is a directive from above that isn't even a framework and isn't up for debate.

Since fintech cannot operate independently, some take matters into their own hands in balancing their business, including reputation, with the risk level they share with other fintech. This is because the regulatory framework is currently far removed from the fintech due to the belief that it only takes a small portion of the transaction.

There is discrimination, no guidance or rules for opening up a government service payment to all fintech, and no application or imposition of the necessary conditions for all participants.

The regulatory bodies must also develop platforms that allow fintech companies to provide input on difficulties, concerns, and existing regulations—many of which lack awareness or are not well-established platforms.

4.3.3 Operational risk Origins (Internal vs External risks)

The majority of them concur that because staff members have more privileges than outsiders, internal danger is greater than external risk. The fintech companies that currently hold licenses from national banks are few and operate on a small scale. In the traditional fintech environment of banks, conversely, operational risk stems from a large number of staff members, high operational intensity, increased technology usage, and insufficient knowledge.

The main risk stems from internal staff running the system and control, which starts with process and compliance, monitoring, ethics, and (process, technological, and human) gaps in technology. Regarding the transaction monitoring aspect, it is also necessary to control the danger arising from technological gadgets.

Fintech needs to be transparent about how it will address frauds resulting from external dangers. As of right now, there are no rules or guidelines in place in the event that internal system issues at banks and mobile money providers produce incidents.

Fintech operators—which can include conventional fintech firms, banks, or even telecoms with mobile money operating licenses—are primarily vulnerable to external threats. Even though the vulnerabilities are being examined at first, the bank's integrations are concerning. Banks are attempting to reduce operational risks by implementing secure APIs in order to mitigate new types of dangers that may arise during operations.

The other risk, which is a hybrid of the first two and arises from both external and internal social engineering fraud, is growing in significance. Another one that needs to be noted as a concern is cyber risk.

Unlike other nations, our operational risk, particularly with regard to fraud, originates domestically because the national currency is the birr. However, it is also undeniable that attempts are being made to deceive other international payment businesses by pretending to be a bank in the country.

4.3.4 Operational Risks and Impact Assessment

Even though everyone acknowledges that operational risk is one of the biggest concerns, urgent, and somewhat manageable, they all believe it to be remote. Furthermore, operational risks—such as system faults and high frequency and low effect—may be less common but have a greater potential impact. For low frequency and high impact operational risks, a robust procedure and evaluation must be in place because they have the potential to bankrupt the fintech and negatively affect the ecosystem.

Concerns about customers or fraudsters impersonating customers are currently being raised more frequently and with less impact. Regarding this, there is a substantial growth in fraud from betting organizations integrating these fintech solutions to the point where it is harming the fintech's reputation.

Customers have reported being phoned by scammers who have access to all of their personal information and who persuade them to provide their password. Following the money transfers made by the scammers, fintech organizations will send their clients a confirmation message. Customers may come to believe that the fintech is the one sending the money as a result of this. In this sense, fintech companies are now working together based only on agreements to assist customers in tracking down transactions, freezing those accounts (although there is no explicit rule regarding the amount of money involved), and forwarding the case to law enforcement for additional investigation and victim help. They are unsure of their exact responsibilities in this regard, as well as those of working with them, and how to maintain their reputation and the trust of their clients.

One of the fintech experienced commission arbitrage; nevertheless, by reserving operational harm, the fintech was able to cover the clients' losses and fix the system. There was ping pong with the bank to reimburse the clients in another event that occurred as a result of integration problems with banks. The regulating body must establish a threshold in this area as well (how many customers suffered, to what extent).

In one instance, a partner ordered a different number from the bank that the customer had not ordered, and the fintech side ended up with the erroneous account. The bank refused to accept responsibility for the event, so the fintech was forced to absorb the loss to avoid harm to its reputation.

The National Bank of Ethiopia steps in to save the banks in the event that such incidences impact deposit mobilization, although it is unclear who will bear the brunt of the losses.

4.3.5 Operational Risk Participants

Even though every fintech operates under the external controlling measures, the fintech ecosystem is interrelated, and an increase in operational risk in one area of the interconnection exposes the other. National Switch, banks, fintech, agents, and customers

are the players in the fintech industry that face operational risks. There believe that the owners of telecom infrastructure should be involved.

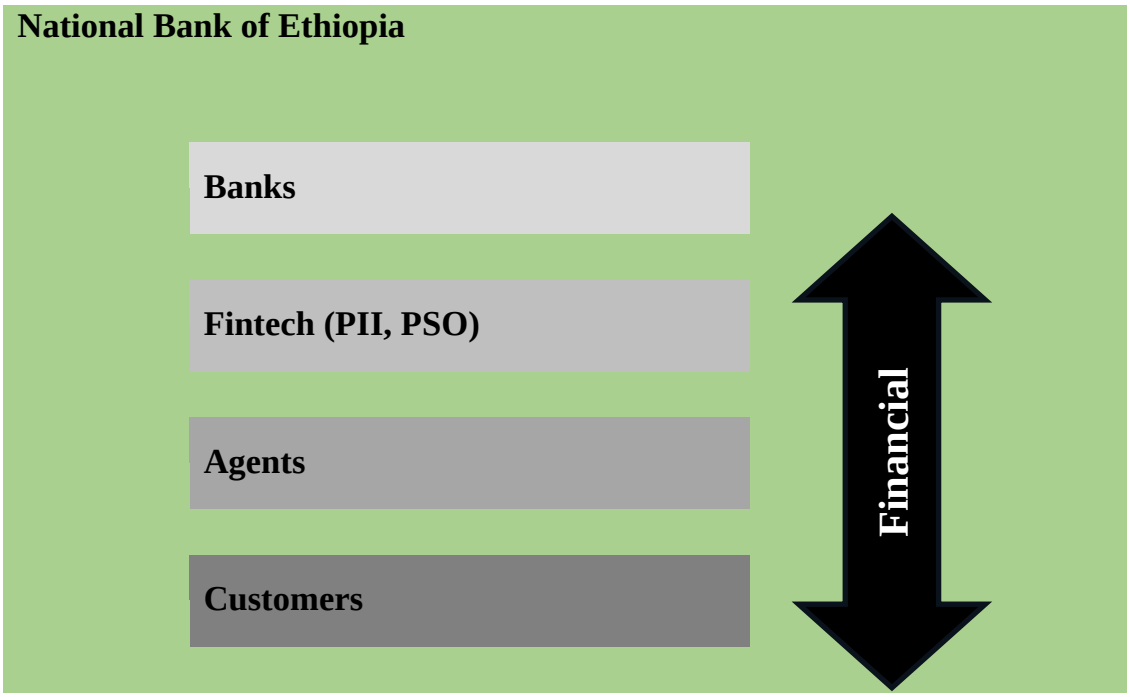


Figure 2:Operational Risk Players

Regarding telecom, the telecom infrastructure serves as the starting point for any digital financial service provider connectivity, and it is imperative that this primary gate has robust controls in place. Then, in contrast to traditional banks, whose networks are internal to the company, fintech businesses want their networks to be expanded to include agent, bank,

and customer networks as well as other fintech networks that are open to the public. Leaving open the possibility of bolstering security and procedures for a particular setting.

Furthermore, it is imperative to establish the extent of liability of platform owners/providers in the event of an incident or damage. Currently, this liability may be found in the company contracts.

4.3.6 Awareness and degree of knowledge

The fact that the regulator is new to this sector puts the players at risk. The regulatory body must have a dedicated division or team and take the initiative to raise awareness, establish the bar for minimum certified experts in the fintech industry, and add value by raising the standard of knowledge that the regulator should set for the industry. The fintech industry presents a challenge to its knowledge domains, as well. Given the privileges that staff members have on the systems, this presents a significant risk that the fintech must address.

Increasing the expertise and awareness of agents and merchants would benefit fintech by giving them an extra hand in protecting and raising client awareness.

The greatest knowledge gap is in the area of customer knowledge since customers are essential to the long-term viability of the company and because every stakeholder and regulator must be aware of the importance of protecting customers.

Operational risk is an industry issue that should not be left to the discretion of individual fintech companies, but rather requires regulatory intervention and oversight. The regulatory body's comprehension that operational risk is a critical concern is questionable.

4.3.7 Fintech Vs. banks' acceptance of current regulations

The majority of fintech companies believes that the current regulations are traditional and should be modified. When we observe banks, we observe that they adhere rigorously to the regulations.

Conversely, fintech originates from the IT sector, emphasizes technology, and lacks strong operational management (Process and others).

4.3.8 What does the regulation have?

The regulatory community has demonstrated a strong commitment to fintech in recent times, as seen by the openness of the market to foreign investment in the environment, the introduction of the QR standard (which coincides with my finalization of this paper), and the PII and PSO directives that further facilitate the industry. They all think that this is just the beginning, and that the regulation needs to be improved upon to reach new heights.

4.3.9 Recommended Industry Best Practice

Industry norms are needed for fintech companies operating in Ethiopia, as they are not currently implemented.

I. System minimum standards: In this market, system norms are less stringent than requirements. The systems' security is subpar (outdated, extremely vulnerable), endangering the environment. Having a minimum standard ensures that everyone is operating at the same minimal level. Furthermore, system security must be regularly checked for strength and infiltration by employing an outside party.

II. Platform availability: This is caused by outages that reduce the dependability of platforms. To mitigate this, proactive 24/7 monitoring is used to identify incidents before they affect customers. Additionally, high availability platforms are deployed for disaster recovery and business continuity plans that are important to the platforms (business critical/mission critical). Furthermore, the systems must have alerts that alert investors to any transactions that exhibit an abnormal trend when compared to the previous day, week, or month without experiencing any incidents.

This helps the companies identify abnormalities that may be the result of fraudulent activity or system errors.
Furthermore, even in cases where platform availability falls within the planned range, customers may experience sporadic service disruptions, which should be taken into account.

III. Fraud: To obtain financial gain, unscrupulous customers, agents, and merchants exploit gaps in platforms and procedures to carry out fraudulent transactions. This is lessened by having adequate fraud controls in place throughout the ecosystem to spot such activity and implement corrective actions. People who use the same password must be subject to strict monitoring and attention, and the length of the password must take into account system controls.

IV. Money Laundering: This refers to the introduction of proceeds from criminal activity into the mobile money ecosystem in order to make them appear legitimate. This is lessened by connecting the mobile money system to appropriate AML platforms, which are able to identify and flag such transactions.

V. Development gaps: Due to them, there may be manual operations or embedded problems, which raises the possibility of operational risk. The fintech must assess these concerns and give a solution.

VI. Decision makers: Decision makers should be accessible at all times, with authority delegation and a well-defined approval process in place for less-than-crisis incidents that must be established and adhered to.

VII. In order to prevent similar situations from occurring to other players in the future, documentation and lessons learned must exist and be shared with the regulating

body. The regulatory body must also establish a platform that can be shared with others.

VIII. Procedures: Describe the procedures. Some businesses let consumers to take advantage of their weak processes. The processes must specify precisely the level of control and who is authorized to access what information from the system. To prevent any gaps, there should also be a smooth procedure for rescinding access when someone moves up in rank.

IX. Culture of Backup - Data backups, whether automatic or manual, must be implemented by businesses in order to minimize data loss. This requirement may vary from business to business, and some may not have backup data at all.

4.3.10 Recommended focus areas for the regulatory

The respondents agree that there are things that are done by the regulatory for fintech to start such as and including Proclamation for PSO is revised which addresses a lot of gaps including opening the business to foreign investors. Licensing and authorization of payment system operators and payment instrument issuers, deposit insurance, Communication Fee, Payment instrument issuer, expanding the mobile wallet, QR payment standardization in addition also Person to Merchant is also in the pipeline.

Also, currently because of the lack of having more regulatory actions the fintech is operating in a risk environment which is expected the regulatory body to consider. Not having good monitoring of operational risks, unclear framework, no money laundry related regulation, no terrorist financing related regulation, no customer privacy, no well-defined operational risk and if defined also not well exercised operational risk, no engagement with fintech, no data protection policy, no clear business risks, no measurement of compliance.

The current framework is generic, and it only mentions companies should have risk management framework, business continuity framework and business continuity plan. In that regard the minimum list that should be considered across all fintech.

And the focus area for the regulator should be having a clear directive, standard, framework, procedure, policies and others based on the suitability on Money laundering, Terrorist financing, System resilience, Data protection, Security such as system to customers, Identity theft, Social engineering, Agent distribution channel validation ,Fraud such as commission arbitrage, Impersonation, Overdraft, Bankruptcy risk, International money transfer, Threshold/level set for the number of customers be impacted and extent, Protecting methods for reputational damage for the fintech to take, Enacting policies that minimize the operational risks, Supporting the ecosystem and in addition

I. Monitoring the businesses appropriately: -Consistent follow-up and monitoring is a need with check points against the set rules and regulations by the regulatory body.

II. Payment of government services: - bring fair playground to all DFS operators to be part of.

III. Penalties for violators for violations and safeguard customers & partners.

IV. Post incident handling, communication and lesson learned for the fintech environment.

V. Remittance in relation to foreign currency is a blocker that should be considered.

VI. Crisis management: - currently few has crisis management including in the IT domains, but others are behind in exercising it and having a regulation on crisis management helps in standardizing across the eco system.

VII. Regulation in relation to sandbox should be there to give flexibility and support innovation in the fintech and in relation to these controlling mechanisms also has to be considered.

Regulatory role is irreplaceable. If the regulatory is strong which is led by knowledge is very important. When it comes to Ethiopia the regulatory, in relation to the digital financial services, mostly donot have the capability in knowledge to lead thing by understanding ahead of the environment. Our regulatory has to be strong and create framework is critical.

Supporting standards like-Customer Privacy -Personal Information Identifier (PII) regulations has to be there, GDPR has to be brought for the environment. Enable the companies on human development. System Assurance involvement for fintech, for example with the main system if all the auxiliaries are there like AML system has to be checks and should be a mandatory from the regulatory.

Continuous awareness and enforcement condition has to be there. Since the environment is new as a country, we have a late comer advantage to mature to a proper operational risk management in place. At the same time also the regulatory has to be couscous of not creating a market where the local investors cannot grow.

In addition to certifying the fintech, if there is a direction from the national bank not to integrate with any uncertified entity otherwise the certificate revocation will happen would help the environment players also to control the environment.

Another aspect is putting insurance for each account has to be though of in implementing in the future which will help in refund when incident happen.

Finally, the operational risk is an aspect that should be controlled and the management to be strengthened from all direction.

CHAPTER FIVE: Conclusion and Recommendation

5.1 Introduction

This study's goal was to evaluate the operational risks that exist now and the function of the regulation and based on that this chapter will have summary, conclusion, recommendation, limitation, and future research areas.

5.2 Summary

The primary goal of the research was to identify the operational risks in digital financial service providers in relation to the implications of the necessary regulatory framework. The following research questions were addressed in the study:

1. What are the prevailing operational risks in Fintech services in Ethiopia?
2. What are the gaps in the current operational risk management regulation?
3. What needs to be added/modified in operational risk management regulations?

Upon reviewing the responses regarding operational risks prevalent in Fintech services in Ethiopia, I found that companies prioritize their risk appetite and have distinct operational risk focus areas. However, they also feel that a minimum risk profile should be established for all companies to exercise, with the option for individual companies to add additional risks on top of that. Based on their responses, it is also discovered that there are operational risks that ought to be routinely addressed. Failure to do so could have an effect on a variety of aspects of the environment, including business continuity plans, measures to address system vulnerabilities, and the implementation of appropriate processes, policies, controlling measures, and security measures. Because of the impact and privilege level, internal operational risk has a greater influence than external risk. When applying changes to systems being followed the proper process, mentioning the incident that happened on Commercial Bank of Ethiopia in March 2024, the impact have a significant effect on the ecosystem unless the systems internally reflect the process that should be followed and create gaps. When incidents happened, there is a proper response plan in place.

Despite being the backbone and sole major player in the fintech industry, banks also pose significant operational risks due to their large transaction volume and traditional brick-and-mortar operations. This is because the fintech industry is still in its infancy and only a small number of companies have entered it.

In connection with this, determining if the existing operational risk management rule has any gaps was the second goal. Regarding this, they are all of the opinion that the regulation is not doing enough to address operational risk in fintech and should be doing more. Fintech companies are required by law to maintain an operational risk registry, however there is currently little oversight or control over this requirement. Even the regulatory agency has a significant knowledge gap, but technology is advancing quickly. Some commentators on fintech point out that the approach is a little directive and that there is no venue to hear their opinions.

There is very little to no platform for fintech to exchange expertise and learn from one another. Some people think it's difficult to maintain their high standards because other fintech companies might not have the same ones, and even if they do pose a risk to the environment, there isn't much oversight or control. Instead, it's up to them to negotiate and volunteer to uphold the standards. In this sense as well, particularly from the system perspective, funding is required to meet the demands made by other fintech companies.

When discussing the areas of operational risk management regulations that the interviewee suggested. In order to minimize operational risk, support the eco system, and appropriately monitor the business, it is expected that the regulatory framework would remain intact. Supporting standards such as GDPR for the environment and Customer Privacy -Personal Information Identifier (PII) legislation must exist. Second, give businesses access to human development resources and establish uniform certifications for staff members and fintech organizations. Fintech system assurance involvement: for instance, the system has all the necessary auxiliary services, such as AML, in place. The regulatory body must have complete backing as it will enact legislation that will protect clients and partners, level the

playing field for all DFS companies, and impose fines for infractions. Sensitization campaigns, forums, and harmonized norms are lacking; regulators must provide these things in order for there to be widespread knowledge and usage. Even if one internal system is as good as another, a partner's vulnerability will still matter. Digital payment risk impacts everyone. Forums are essential for exchanging best practices and learning new ones. In order to provide certification and standard compliance, evaluation is also required.

Every fintech company should be able to adhere to criteria that prevent prejudice in the government payment services. Having a guide on the rules and procedures for incident and change management on systems, the escalation path, communication, and decision-making is also helpful. Fintech-specific norms and regulations must be in place, and if needed, a division between fintech and banks must be made.

It's time for sandboxing and deposit insurance. PSO and PII management. There must be risk management, a minimal requirement, ongoing knowledge, and enforcement requirements. System warnings, trend comparisons, and lesson learned documentation are essential for operations and post-event documentation in fintech organizations, and these are areas where regulators should focus their efforts.

They all agree that regulations play an indispensable function and that, given our nation's late-comer advantage, regulations may develop more readily.

Given the fintech industry's dynamism and reliance on technology, National Bank of Ethiopia is well-positioned to lead, advise, and control the sector in relation to operational risk. Indeed, the bank has extensive experience in this area and should take the lead in enforcing existing regulations, advising the Fintech environment, and meeting industry demands. Every fintech company should be mindful of operational risk and implement controlling mechanisms such as KPIs and appropriate processes, according to the suggestions made by all. Furthermore, how the business continuity strategy is implemented after the issue must be there to support fintech in their quick recovery.

Most of them concur that the lack of a platform to sandbox fintech companies' innovations and ideas is impeding the industry's ability to thrive.

Fintech companies have been tasked by the regulatory body to be truthful with-it regarding cases of little and big financial loss because of loss operational risk management.

In summary,

- Fraudsters (internal and external) who take advantage of the gaps is another prevailing operational risk that the regulatory body has to closely monitor, Key Performance Indicators must be there for each digital financial services measure the performance.
- The focus of digital financial service providers on the platforms they use for delivering the services have to be enabled to the level in closing the operational gaps.
- Having minimum certification standards for the digital service providers to fulfill and continue, and making this as a requirement for integrating with other fintech has to be a requirement for synchronization of the environment and harmonization. To identify gaps in the current operational risk management regulation.
- Acquiring the basics operational risk management standards being followed by digital financial service providers in other countries as a baseline.

5.3 Conclusion

This study evaluated whether fintech, or individual digital financial service providers, should be in charge of operational risk management. The literature research demonstrated the significant consequences of improperly managing operational risk, as well as the challenges associated with gathering information to estimate damage and create a consistent list for assessing operational risk. Due to the aforementioned factors as well as the research's findings, regulations ought to provide a framework and assistance in establishing a harmonized environment.

5.4 Recommendation

According to the study I recommend the regulator's job is to establish a coordinated understanding among industry participants for the improvement of the ecosystem. The regulatory body needs to adopt a cooperative approach instead of a dictatorial one.
Rather than leaving it to the internal operations of the fintech company, the regulator has a deeper degree of analysis of operational risk to have a common minimal list that should be exercised across the environment.

- At regulatory level there are policies that to standardize and harmonize the environment pre and post operational incidents.
- Create fair playground and do the monitoring and the control in a uniform way across all the digital service providers.
- Create a platform for a review, feedback, and discussion among the digital service providers for a suggestion, concern and objection to be raised and addressed.

5.5 Limitation

Because fintech is relatively new in the nation, the interviewee's awareness level is occasionally questioned which causes the response to fluctuate.

The answers I received now might not align in the future due to a change in the environment because there have been modifications to the regulations pertaining to directives, standards, and other things.

5.6 Future Research

If operational risk management can be left to individual firms or requires a structured strategy from the regulating body, more study can be conducted. Furthermore, every fintech company should strive towards achieving a minimal operational risk registry, with the opportunity to choose other risks at their discretion.

Furthermore, employees, upper management, and the regulator do not possess the necessary level of fintech awareness. The academic setting will benefit from research on the degree of awareness in the fintech sector.

Furthermore, while having a strategy is one thing, how often it is practiced and if it is improved upon over time is another topic of research, particularly in post-event and business continuity plan.

References

Abel, G. (2023). Characterizing Mobile Banking Transaction Fraudulent Activities. Un published MBA thesis, Addis Ababa University.

Arkanuddin, M. F., Saragih, F. D., & Nugroho, B. Y. (2021). The Key role of the Financial Regulation in FinTech Ecosystem: a model validation. *Estudios De Economía Aplicada*, *39*(12). https://doi.org/10.25115/eea.v39i12.6239

Alshari, H. A., & Lokhande, M. A. (2023). The relationship between the risks of adopting FinTech in banks and their impact on the performance. Cogent Business & Management, 10(1). https://doi.org/10.1080/23311975.2023.2174242

Aroda, P. (2016, November 25). Essays in Quantitative Risk Management for Financial Regulation of Operational Risk Models. Retrieved from https://yorkspace.library.yorku.ca/items/16a2758f-df33-414c-bccb-4afedb0a6d05

Barriga, L., & Rosengren, E. S. (2006). Overview of operational risk management at financial institutions. In Elsevier eBooks (pp. 119–133). https://doi.org/10.1016/b978-008044949-4/50041-6

Bank Risk Management Guidelines (Revised), May 2010

Berhane, S. (2022, June 7). Federal police warns increase in mobile banking fraud | The Reporter | Latest Ethiopian News Today. The Reporter Ethiopia. Retrieved from https://www.thereporterethiopia.com

Chen, J. (2022, April 27). Basel Accords: purpose, pillars, history, and member countries. Retrieved from https://www.investopedia.com/terms/b/basel_accord.asp

C.R. Kothari (2004). Research Methodology Methods and Techniques.

Crawford, J. (2017). Regulation's Influence on Risk Management and Management Control Systems in Banks. Regulation's Influence on Risk Management and Management Control Systems in Banks. Retrieved from http://uu.diva-portal.org/smash/record.jsf?pid=diva2%3A1151290

Crisanto, J. C. (n.d.). Big techs in finance: regulatory approaches and policy options. Retrieved from https://www.bis.org/fsi/fsibriefs12.htm

Eceiza, J., Kristensen, I., Krivin, D., Samandari, H., & White, O. (2020, April 13). The future of operational-risk management in financial services. McKinsey & Company. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-future-of-operational-risk-management-in-financial-services#/

Ethiopia's National Digital Payments Strategy 2021-2024

FDIC: Federal Deposit Insurance Corporation. (n.d.). Retrieved from https://fdic-search.app.cloud.gov/

Fortune. (n.d.). The banking industry battles festering fraud as clients swindled savings. Retrieved from https://addisfortune.news/banking-industry-battles-festering-fraud-as-clients-swindled-savings/

Ganpat, K., & Harrypersad, N. (2018). Combatting Operational Risk through Regulatory Technology.

George, T. (2023, June 22). *Types of interviews in research | Guide & Examples*. Scribbr. https://www.scribbr.com/methodology/interviews-research/

Gurrea-Martínez, A., & Remolina, N. (2020). Global challenges and regulatory strategies to Fintech. *Social Science Research Network*. https://doi.org/10.2139/ssrn.3576506

HeinOnline. (2024, January 12). About - HeinOnline. Retrieved from https://heinonline.org/HOL/LandingPage?handle=hein.journals/sdintl19&div=16&id=&page=

International Monetary Fund. Statistics Dept. (2020b). The Federal Democratic Republic of Ethiopia: Technical Assistance Report-Financial Soundness Indicators Mission. IMF eLibrary. https://doi.org/10.5089/9781513564876.002.A001

Izhar, H. (2012). *Modelling operational risk measurement in Islamic banking: a theoretical and empirical investigation* (Doctoral dissertation, Durham University).

Kwon, Y., Lee, J., & Owens, J. (2023, May). Managing fintech risks. *ADB Briefs*. https://doi.org/10.22617/brf230170-2

Kyrtsis, A. (2009). Shifting contracts, operational risk, and regulatory mythologies. *Shifting Contracts, Operational Risk, and Regulatory Mythologies*. Retrieved from https://www.bi.no/InstitutterFiles/JB_Three_keynotes_ms.pdf

Mahalle, A., Yong, J., & Tao, X. (2021). Regulatory Challenges and Mitigation for Account Services Offered by FinTech. *Regulatory Challenges and Mitigation for Account Services Offered by FinTech*. https://doi.org/10.1109/cscwd49262.2021.9437631

Meshack, K. M., & Mwaura, R. W. (2016). THE EFFECT OF OPERATIONAL RISK MANAGEMENT PRACTICES ON THE FINANCIAL PERFORMANCE IN COMMERCIAL BANKS IN TANZANIA. American Journal of Finance, 1(1), 29. https://doi.org/10.47672/ajf.83

Nikolopoulou, K. (2023, June 22). *What is purposive sampling? | Definition & Examples*. Scribbr. https://www.scribbr.com/methodology/purposive-sampling/#:~:text=In%20purposive%20sampling%2C%20you%20set,on%20a%20relatively%20small%20sample.

Nsaibi, M., Abidi, I., & Rajhi, M. T. (2020). CORPORATE GOVERNANCE AND OPERATIONAL RISK: EMPIRICAL EVIDENCE. International Journal of Economics and Financial Issues, 107–115. https://doi.org/10.32479/ijefi.9861

Parfenova, A. (2016). The effects of regulations on risk management within the Swedish Banking Sector. Retrieved from https://www.diva-portal.org/smash/record.jsf?dswid=-2110&pid=diva2%3A947318

Pepi, M. (2019). Operational Risk Management in a Financial Institution. *Ovidius University Annals, Economic Sciences Series*, *19*(2), 840-849.

Philippon, T. (2017, August 7). The FinTech opportunity. Retrieved from https://www.bis.org/publ/work655.htm

Power, M. (2005). The invention of operational risk. Review of International Political Economy, 12(4), 577–599. https://doi.org/10.1080/09692290500240271

Regulatory treatment of operational risk. (2001, September 28). Retrieved from https://www.bis.org/publ/bcbs_wp8.htm

Sherwood, J. (2018, March 27). Operational Risk - Key Problems with the Advanced Measurement Approach - The Global Treasurer. Retrieved from https://www.theglobaltreasurer.com/2005/04/25/operational-risk-key-problems-with-the-advanced-measurement-approach/

Shri Shaktikanta Das, Governor, Reserve Bank of India, Keynote Address delivered at the NITI Aayog's FinTech Conclave, Delhi on March 25, 2019.

Solutions, S. B. (n.d.). Liberalization of the digital financial services to foreign Direct Investment | Aman & Partners Legal Service LLP. Retrieved from https://www.aaclo.com/insight/liberalization-of-the-digital-financial-services-to-foreign-direct investment/#:~:text=The%20approval%20and%20ratification%20of,(mobile%2Dmoney)%20sector

Sturm, P. (2013). Operational and reputational risk in the European banking industry: The market reaction to operational risk events. Journal of Economic Behavior and Organization, 85, 191–206. https://doi.org/10.1016/j.jebo.2012.04.005

System of National Accounts. (n.d.). Retrieved from https://unstats.un.org/unsd/nationalaccount/glossresults.asp?gID=340#:~:text=A%20monetary%20transaction%20is%20one,stated%20in%20units%20of%20currency.

Thematic Research in Qualitative Research - QualTricS. (2023, June 16). Qualtrics. https://www.qualtrics.com/experience-management/research/thematic-analysis-in-qualitative-research/#:~:text=Thematic%20analysis%20involves%20initial%20analysis,and%20even%20transcribing%20the%20data.

Uña, G. (2023). Fintech Payments in Public Financial Management: Benefits and risks. *IMF eLibrary*. https://doi.org/10.5089/9798400232213.001.A001

Yohannis, F. (2021).The effect of risk management on financial performance: the case of commercial banks in Ethiopia

APPENDIX I

Interview Questions

SCHOOL OF GRADUATE STUDIES

MASTER OF BUSINESS ADMINISTRATION PROGRAM

Questionnaire to be filled only by Fintech Company

Dear Respondent

My name is Mahlet Tsegaye, and I am currently a Master of Business Administration (MBA) student at the College of Business and Economics, Addis Ababa University (AAU). This questionnaire aims to identify the Digital Financial Services and Operational Risks in Ethiopia: Implications for the Necessary Regulatory Frameworks. I would like to assure you that the information you provide will be used only for research purposes and kept confidential. Your genuine responses are regarded as a great input to the quality of the research outcomes.

Thank you in advance for your participation.

General Information

Please select the right answer to the best of your knowledge.

For questions that require your further opinion, please respond clearly and faithfully.

For any queries – Mob. 0911131564 or E-mail: mahitseg@gmail.com

Interview Questions for Fintech Companies

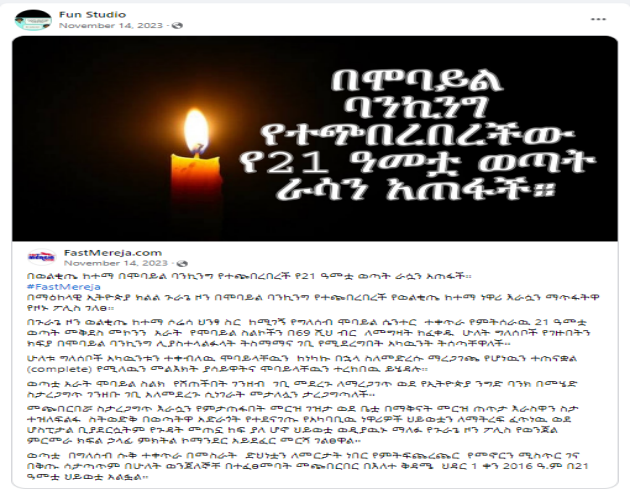
1. What are the present operational risks and how are they being addressed? (Is there a clear agreed upon industry list, the way to calculate) Does operational risk has a new classified category?
2. Out of the players in the mix (Banks, Regulators, Agents, Fintech, Customers), whose side are these operational risks happening on and by whom?
3. Have there been instances where operational risks took place and there was no clear regulatory guide on who should pay for the loss or damage? Can you elaborate on it with a case, please?
4. Are there any operational risks that require greater attention than others? If that's the case, can you tell me about them?
5. Is the frequency of occurrence known for operational risks such as staff misconduct, transaction errors, wrong transfers, and others?
6. What is your view on the significance/need of the regulatory body to support in reducing operational risks?
7. What is your assessment of the current regulatory framework for operational risk?
8. What are the regulatory approaches that have been created to address these risks? Is there a regulatory capital requirement set in place?
9. Can you give me an overview of recently issued regulations that are influencing how fintech risks are managed?
10. Do you have any operational risk areas where you would like regulations and guidelines in the future?

Interview Questions mapped to the research questions and specific objectives.

Research Question	**Specific Objective**	**Interview Question**
What are the prevailing operational risks in Fintech services in Ethiopia? What are the gaps in the current operational risk management regulation?	To identify the prevailing operational risks in Fintech services in Ethiopia. To determine the specific operational risks that need higher focus.	What are the present operational risks and how are they being addressed? (Is there a clear agreed upon industry list, they way to calculate) Does operational risk has a new classified category?
		Out of the players in the mix (Banks, Regulators, Agents, Fintech, Customers), whose side are these operational risks happening on and by whom?
		Have there been instances where operational risks took place and there was no clear regulatory guide on who should pay for the loss or damage? Can you elaborate on it with a case, please?
		Are there any operational risks that require greater attention than others? If that's the case, can you tell me about them?
		Is the frequency of occurrence known for operational risks such as staff misconduct, transaction errors, wrong transfers, and others?
What are the gaps in the current operational risk management regulation? What needs to be added/modified in operational risk	To determine the specific operational risks that need higher focus. To added/modified in operational risk management regulations.	What is your view on the regularization of operational risks?
		What is your assessment of the current regulatory framework for operational risk?
		What are the regulatory approaches that have been created to address these risks? Is there a regulatory capital requirement set in place ?
		Can you give me an overview of recently issued regulations that are influencing how fintech risks are managed?

management regulations?		Do you have any operational risk areas where you would like regulations and guidelines in the future?

ANNEX 1:



Source: Social Media (Facebook), 2023