UNIVERSITY OF NAIROBI

COLLEGE OF BIOLOGICAL AND PHYSICAL SCIENCES

SCHOOL OF COMPUTING AND INFORMATICS

DIGITAL LENDING: STRENGTHENING TECHNOLOGY RISK MANAGEMENT IN MOBILE MONEY LENDING

GEOFREY NYAMARI OGOTI

REG NO: P54/6142/2017

SUPERVISOR: CHRISTOPHER A. MOTURI

A Research Project Submitted in Partial Fulfilment of the Requirement for the Award of the Degree of Master of Science in Information Technology Management,

School of Computing and Informatics, University of Nairobi

June 2019

DECLARATION

This research is my original work and has not been submitted for a degree in any other university.

Signature: ______________________________ Date: ____________________

This project report has been submitted in partial fulfilment of the requirement of the Master of Science Degree in Information Technology Management of the University of Nairobi, with my approval as the University supervisor.

Signature: ______________________________ Date: ____________________

Christopher A Moturi
Director
ICT Centre
University of Nairobi

ACKNOWLEDGEMENT

I would like to express my deepest gratitude to my supervisor, Mr. Christopher A. Moturi for his guidance throughout this research. His dedication to service, teaching and instruction is admirable. His support and motivation throughout is very much appreciated.

I would like to also thank my lifelong friend Mutheu for her additional review and feedback. My family has also been of great help, I thank them for their support.

Throughout this research, there are many others who have been very supportive. I would especially like to thank the mobile lending professionals who reviewed my research objectives and provided feedback on an on-going basis.

ABSTRACT

Background

There has been a push by financial institutions to achieve a competitive advantage by offering innovative products in the marketplace, one such product is mobile money lending.

Purpose

The purpose of this research was to strengthen the capacity of technology risk management by proposing practices and strategies that can help mobile lending institutions.

Method

Using the RiskIT framework, data was collected in January 2019 using questionnaires. The respondents included professionals in Mobile Lending, Information Systems Audit, Credit, Risk and Information Security. The entities included five Central Bank of Kenya licensed mobile money lenders and five unregulated mobile lenders based in Kenya.

Findings

The study shows that compared to unregulated entities, regulated digital credit providers have robust technology risk management environments where IT risk is understood and monitored. For unregulated entities, there are weaknesses in technology risk evaluation and response.

Limitation

The research was limited to the top lenders in regulated entities and additional unregulated lenders. Therefore, respondents from other tiers of banking were left out. Further, the location of all the respondents was Kenya's capital, Nairobi.

Value of Research

In effect, this research contributes to efforts of the country and the national government on having a secure and strong financial system that contributes to the Millennium Sustainable Development Goals (SDGs). In addition, a trusted financial system is key in enabling an ecosystem for growth of the President's Big Four Agenda.

Conclusion

It is proposed that entities that offer mobile money lending be cognizant of the requirements that ensure borrowers and the lending ecosystem is protected from technology risks that could materialize. Digital lending regulation and continuous monitoring through data & analytics is one avenue through which such risks could be mitigated.

Key Words: Mobile Money Lending, Technology Risk Management, RiskIT Framework, Mobile Applications, Mobile Regulation, Digital Lending.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

CISA – Certified Information Systems Audit

COBIT – Control Objectives for Information and Related Technologies

CBK – Central Bank of Kenya

IAS39 – International Accounting Standard 39

ICT – Information Communication Technology

ISACA - Information Systems Audit and Control Association

IFRS – International Financial Reporting Standard

KYC – Know Your Customer

RiskIT – Risk IT Framework by Information Systems Audit and Control Association

SME – Small and Medium Enterprises

CHAPTER ONE

INTRODUCTION

1.1 Background

In the recent past, the East African financial marketplace has experienced growth in technological innovation. Being a frontier market that has potential for more, getting technology risk management wrong could have costly effects in the short term and long term (Miled & Rejeb, 2015).

It's been seen through studies that digital credit is a contributor to economic value and growth in the developing world. This is because it offers access to credit to individual and small enterprise consumers. (International Finance Corporation, 2018). Digital lending is critical for demonstrable reasons, for example, restricted access to inexpensive credit limits the ability of families to invest in activities such as farming, education and small business. When this happens, it hampers much needed economic growth and development for frontier markets (Griffith-Jones, Karwowski, & Dafe, 2014)

One particular enabler of digital lending is mobile money. The introduction of M-PESA in Kenya has had positive socio-economic effects; for example, mobile money enabled digital lending has been associated with growth of businesses and poverty alleviation in Eastern Africa (Klapper, 2016). Mobile financial services is viewed by researchers as the future to improving digital credit and access in the developing world (GSMA, 2016)

In November 2012, Safaricom (www.safaricom.co.ke), a leading telecommunication services provider in Kenya, launched M-Shwari (Alliance for Financial Inclusion, 2012), a digital lending platform that leverages mobile and telecommunications data for loan rating and processing. M-Shwari transactions are in thousands of loan applications daily. (Blechman, 2016). The current digital lending platforms in the region include: M-Shwari by Safaricom and CBA, M-Bank by KCB, Zidisha, Branch, Kiva, Tala, MoKash, Eazzy Loan by Equity Bank (Totolo, 2018), among others.

Digital lending refers to using digital means to process loans and advances directly to customers including SMEs (small to mid-size enterprises) (Beck, Demurgic-Kunt, & Martinez, 2007).

Digital credit processing would automate some if not all components of the lending process. Advanced analytic models automate credit decisions for faster, more precise and targeted underwriting (Almari, 2002) which enables lenders to deliver services more efficiently while retaining their traditional process practices.

In modern age, businesses work in highly dynamic environments. Technology risks are probabilities of exposure in technology assets that could lead to loss (Ahlan, 2012). Companies have controls in place to govern risks but a significant deficiency in internal control should merit our attention. (Ahlan, 2012).

For example, when emerging technology or ICT regulations come into effect, they pose a risk to organizations and continuous monitoring and responses need to be agile (Institute for Internal Auditors, 2007).

1.2 Problem Statement

There are weaknesses in the technology risk governance, evaluation and response strategies that digital lenders have applied that have in turn led to exposure to technology risks.

In the East Africa region where there has been a rise in digital lending, defaults and losses in revenue associated with digital lending have been higher than other lending categories (Central Bank of Kenya, 2017). These losses can be attributed to poor technology risk management practices.

In most cases (Francis, Blumenstock, & Robinson, 2017), digital lenders do not have a face-to-face interaction with their borrowers, this exposes the lending market to a variety of risks; some that are associated with money laundering and cross border terrorism. This presents a risk of reputation challenges as aggrieved customers could publicly challenge the products of a lender (Aduda & Gitonga, 2011). Some of the results of unmitigated technology risks are reputation damage and loss of public trust that ultimately leads to loss of business (Ahlan, 2012).

The technology risks can be managed through technology enabled credit scoring, however, these strategies have not been efficient. This is more so applicable in the case of the Eastern Africa region, where credit scoring is not as developed to the comprehensive detail of individuals, house units or families (Consultative Group to Assist the Poor (CGAP), 2017).

In addition, information sharing and know-your-customer strategies in the East Africa region are not developed to the extent required to enable a robust digital rating ecosystem (Francis, Blumenstock, & Robinson, 2017).

The consumers who support the digital lending ecosystem also find themselves in a place where they do not fully appreciate the loan terms they sign up for and instead would take up credit to deal with most immediate need (McKee, Kaffenberger, & Zimmerman, 2015).

1.3 Research Objectives

The objectives of this research project were as follows;

i) Identify technology risk management practices in entities that offer mobile money lending.

ii) Assess adequacy of technology risk management in regulated and unregulated digital lending environments

iii) Propose appropriate strategies that would help mitigate the risks associated with technology enabled lending.

1.4 Justification for the Study

This research reviews the current state of digital lending in Kenya in order to propose strategies that could strengthen technology risk management in mobile money lending.

Mitigation of risks is an important cornerstone of economic growth supported by financial technology. By mitigating risks associated with mobile money lending, the intended purpose of a strong financial technology ecosystem is achieved and consequently, the economic development agenda is realized. For digital lenders, this research will be useful as analysing the adequacy of technology risk management on the digital lending business helps enterprises better plan and be prepared for a market that demands more and ecosystem that has dynamic emerging risks.

Closely related to the above, in an environment of evolving regulatory reporting requirements, this study will also prove essential in assessing transparency and prudency of digital lending. New reporting standards demand much more from regulated lenders and a proper reporting strategy for any digital lender is critical. This strategy would be backed by systems and technologies that are well designed and fit for purpose.

CHAPTER TWO

LITERATURE REVIEW

This chapter provides a review of various contributions and thought leadership from technology researchers and scholars on the relationships between digital lending, people, economic development, know your customer strategies, credit scoring, technology risks and expected credit losses in financial reporting.

2.1 Digital Lending

The move from manual entry of transactions in a ledger copy was a major breakthrough in payment systems (Ali, Barrdear, Clews, & Southgate, 2014). This has enabled financial technology and innovations like digital lending to grow and embed themselves in the core financial services infrastructure.

While there certainly is some innovation in digital lending platforms, the core processes differ little from traditional lending. The use of technology to manage costs and fast-track lending processes has created an advantage in that it allows institutions to grow their product base efficiently while at the same time, being cost conscious (Allen, et al., 2013).

Based on World Bank research in the Global Findex (World Bank, 2017), Sub-Saharan Africa is a leader in the number of accounts for mobile money, further, research presented by the (Savings Groups Information Exchange, 2016) shows that 18 million people across Eastern Africa region are investing and saving up to 450 million dollars in a year, this shows great potential and opportunity.

This saving culture has led to an increase of business activities and financial access. It can be argued that the growth of mobile financial services in this region has led to accelerated financial ability for families and the growth of regional economy (Mbiti & Weil, 2014). This has been made possible through savings and transaction enablement for SMEs (Allen, et al., 2013). Financial service providers are now able to lend to individuals and to SMEs with evaluation of lending risk, collateralization and relationship management all done through digital platforms.

2.2 Technology Risk Management in Digital Lending

In recent times, the trend of the economic globalization enabled by technology is increasingly evident. All financial technology practitioners take information technology as a necessary condition for survival in the future and the core of their competition advantage (Li & Yang, 2016)

Most of the work done in managing technology risk is aimed at operational and compliance risk (Ahlan, 2012). It is noteworthy that information technology risks pose more threats to organisations in various risk categories that would include; organisation, project, operational, technical, data and information security, and human risk (Ahlan, 2012).

ISACA (Information Systems Audit and Control Association, 2017), an international technology risk professionals association; defines technology risk management as the careful and keen procedure of identifying technology vulnerabilities and potential threats to the technology resources within an enterprise. It further states that deciding what actions, where applicable, to take in managing the identified risk to an acceptable level is a key process in technology risk management. In making the decision, an assessment of the value of the ICT resources to the organization is documented.

In lending, organisations have to face challenging and increasingly new threats from ICT risks in more sophisticated manners. One particular area for example is weaknesses in information sharing. Proper risk management has to be considered in light of regulatory scrutiny to ensure that customer data that is used in scoring is not leaked or lost (Fosu, 2014).

In our fast changing world, management of technology risks can ensure a company has a competitive advantage over the other. Scholars have found that implementation of information security as one way of managing technology risk is a must for organisations in order to maintain and improve their competitiveness. (Dombora, 2016)

2.3 People, Economic Development and Poverty Reduction

There are many motivating factors for lenders to go into business in any geography. Researchers have found evidence that shows lenders do prefer borrowers who are geographically close or customers with similar cultural tendencies (Burtch, Ghose, & Wattal, 2013). While this works well strategically for some lenders, it begs an important question as to whether the benefits or advantages are mutual.

There is evidence of positive impact of digital credit on economic growth (Alliance for Financial Inclusion, 2012). Countries in the developing nations have had policy initiatives that are geared towards implementing strategies to further digital credit growth and reduce any bottlenecks associated with usage of digital lending platforms. (Allen, et al., 2013). In an environment of government policy support and technology ecosystem growth, significant strides can be made.

One such stride is the contribution of mobile money lending to millennium sustainable development goals of alleviation of poverty (United Nations, 2015). This contribution is however only possible if the people agenda is a top priority for all lenders. Ensuring that customers get credit that furthers development and growth in their lives as opposed to debt accumulation is a key success factor.

For example, with the discovery of sports gambling and betting platforms by the youth in the Eastern Africa region, a concern is to what extent do mobile money lenders abet the practice of irresponsible gambling? Research has linked the access to mobile credit and online betting network presence as a contributor to increased gambling among university students in the Eastern Africa region (Korros, 2016).

2.4 Rating Customer's Creditworthiness – Technology Perspectives

Digital lending practitioners use closely guarded models to evaluate and process loans (Almari, 2002). These models are considered competitive advantage in the mobile lending industry. They use a variety of means to ensure that a loan is evaluated based on accurate probabilities of default for different segments and scenarios (Aduda & Gitonga, 2011).

It has been said that credit scoring, despite its shortcomings, can help answer some key questions related to digital lending. Many of the developing nations do not have mature credit bureaus and for those that do, the process of customer evaluation is not robust (Aduda & Gitonga, 2011). In addition to this, (Almari, 2002) has argued that some key questions on optimal evaluation methods have not been yet answered conclusively by a majority of customer rating algorithms.

In developed countries, credit scoring is reasonably established since there is integrated information processing (West, 2000). In less developed or developing countries, information and the extent of use of credit scoring practices is limited. (Aduda & Gitonga, 2011)

2.5 Knowing Your Customer (KYC)

The process of know your customer involves verifying a customer's true identity by requesting for submission of documents that are acceptable as proof. In Kenya, the Proceeds of Crime and Anti-Money Laundering Act (Government of Kenya, 2009) was effected on June 28, 2010 and requires that institutions must "make all efforts to maintain customer records and verify customer identity". Internal reporting procedures are also expected to be robust and aligned to regulatory expectations.

This process is absolutely critical as it creates trust and provides lenders with an opportunity to understand their client base. Compulsory details required include proof of physical address, valid passport, ID card, utility bills, employer letters, personal identification number or driving licenses. In some cases, introduction or verification of details by an existing customer becomes necessary. (Njagi, 2009).

In Kenya, Microfinance Institutions are ready for e-banking and the customer requirements that come with it (Kalui, Muketha, Tarus, & Moturi, 2017), the same needs to be investigated for digital lending practitioners in light of new regulatory requirements for financial reporting.

2.6 Regulatory Reporting on Defaults

The approach taken by financial institutions to determine losses on bad loans under the IAS 39 guidelines was among the factors that contributed to the global financial crisis of 2008 (Can & Gansmann, 2015)

The IAS 39 accounting standard's incurred loss model had several shortcomings, one notable one was the fact that credit losses were not accounted for until there was demonstrable evidence of impairment. The delayed recognition was cited as a major weakness of the impairment model (too little too late). In July 2014, the International Accounting Standard Board (IASB) issued a new reporting standard (IFRS 9) that requires reporting on expected losses or defaults across the lifetime of loans. In the new reporting standard, one key challenge that financial institutions have to contend with is the incorporation of forward-looking macroeconomic data like GDP and lending rate into their credit processes. (The Global Public Policy Committee, 2016)

These require institutions to build models that take into account factors that could affect probability of default. Institutions will need to consider current modelling capabilities, systems and processes in place as well as the availability of timely data pertaining to macroeconomic indicators.

Of critical importance and in relation to digital lending, (Adem, Gichuhi, & Otieno, 2012) established that institutions must ensure a strong governance and controls framework over default estimation and reporting, focusing on data integrity and model validation given the large population of data, models and systems that either did not previously exist or were not used in financial reporting.

Detailed credit scoring would depend on the data captured in technology platforms and the modelling perspectives must be automated and be forward looking. (The Global Public Policy Committee, 2016)

2.7 Research Framework Literature

In this research, there is a diverse selection of theories and studies on technological innovations and risk management.

Based on the study objectives, the most common theories that researchers have used to investigate technology innovation and risk management are the Risk IT Framework from ISACA (ISACA, 2009), the Technology-Organization-Environment (TOE) framework (Tornatzky & Fleischer, 1990) and the Diffusion of Innovation (DOI) (Rogers, 2003).

This research focuses on technology risks associated with digital lending. To thoroughly review this, we have to keenly study why firms take up or implement technological advancement processes in their business environments. The technology-organization environment (TOE) framework introduced by (Tornatzky & Fleischer, 1990) has found scholarly support for factors such as organizational readiness and external competition or regulatory pressure (Iacovou, Benbasat, & Dexter, 1995). The Diffusion of Innovation (DOI) (Rogers, 2003) framework has also found support that relative advantage, compatibility, and observability have a positive influence on the adoption of mobile financial services (Al-Jabri & Sohail, 2012).

The Risk IT framework by ISACA (ISACA, 2009) however is the most relevant to this study for a number of reasons. ISACA's Risk IT framework, is purposed on helping organizations manage technology risk. The framework was developed through wide consultation and is based on the extensive experience of a global team of technology experts, it is based on the principles of similar frameworks such as COSO ERM2 and AS/NZS 43603.

2.8 Proposed Framework for Study and Justification

The Risk IT framework by ISACA was applied for this study based on the research objectives. The process model group activities into three domains of governance, evaluation and response.

Based on the review of the theories and the context of this research, a recommendation of the applicable framework to use is supportable. The relationship between risk governance, risk evaluation, risk response and digital lending is a subject worthy further exploration (ISACA, 2009).

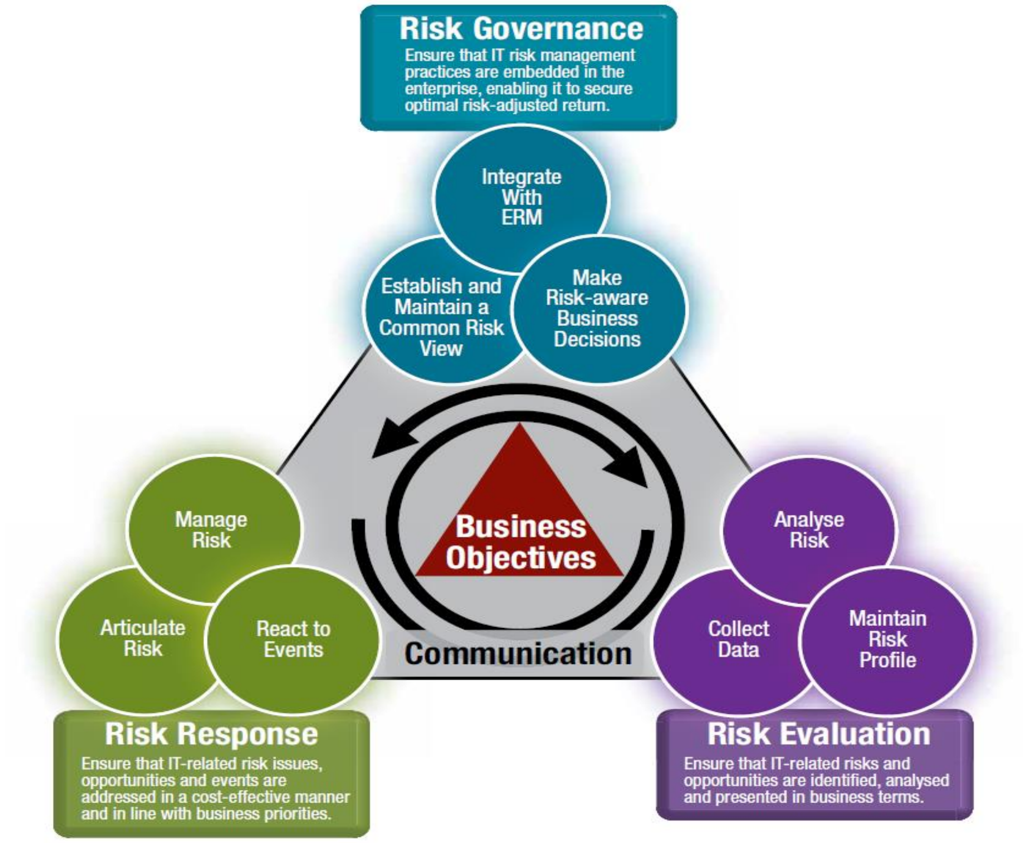

Risk Governance
Ensure that IT risk management practices are embedded in the enterprise, enabling it to secure optimal risk-adjusted return.
Integrate With ERM
Establish and Maintain a Common Risk View
Make Risk-aware Business Decisions
Business Objectives
Communication
Manage Risk
Articulate Risk
React to Events
Risk Response
Ensure that IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities.
Analyse Risk
Collect Data
Maintain Risk Profile
Risk Evaluation
Ensure that IT-related risks and opportunities are identified, analysed and presented in business terms.

Figure 1: Proposed Framework. Source: (ISACA, 2009)

2.8.1 The Risk Governance Perspective in the Technology Lending

The risk governance perspective focuses on key areas of ICT risk, these are tolerance, awareness and communication, appetite, accountability and culture. (ISACA, 2009).

In this study, it is recognized that an organization’s technologies are key assets as they set the rate at which change and adaptability in a firm can happen (Zhu et al. 2006). In light of this, proper risk governance of all the resources an organization has are key to ensure adaptability in a competitive environment that does not allow for error. The resources can be linked to people, process or technology.

In review of literature, a well-managed risk governance structure ensures that all innovation gaps within a firm are filled to influence greater rate of growth. (Dwivedi, Nripendra, Anand, Clement, & Williams, 2017)

2.8.2 The Risk Evaluation Perspective in Digital Lending

The Risk IT Framework advises that meaningful ICT risk assessments require expression in unambiguous terms that can be understood by management.

In digital lending, one way of risk evaluation is through credit scoring. In this research area, correctly quantifying the credit-risk of a customer is the starting point of acquiring a competitive advantage.

The process of technology risk evaluation is not an individual team task. According to the Risk IT Framework (ISACA, 2009), it is important to establish the synergies between the credit department and the technology, risk and marketing teams. Lending has to be evaluated critically by the risk teams and in product development, proper marketing strategies would need to be in place to position the digital credit product in the market and to ensure there is a robust business strategy that delivers the product.

2.8.3 The Risk Response Context

Based on ISACA's Risk IT framework (ISACA, 2009), ICT risk response activities involve risk avoidance, mitigation, sharing and/or acceptance.

Risk avoidance would mean ensuring exit from the conditions that give rise to technology risk while acceptance would mean that no action is taken in response to a risk since a loss is acceptable within defined parameters (ISACA, 2009).

Volatile conditions in market and competition has been known to force firms to use various forms of innovation and response. For example, in the context of credit regulation, government constraints may lead to: increasing costs of doing business, and a rise in compliance requirements of systems or mandatory criteria for the use of these systems in financial services (Sinha, 2012), this would in turn force mobile financial technology institutions to respond while ensuring ICT risks associated with specific market responses are mitigated.

2.9 Conceptual Framework and Research Hypothesis

The three domains of the framework can be shown in the Figure 2 below. The illustration argues that a relationship exists between each domain and adequacy in technology risk management.

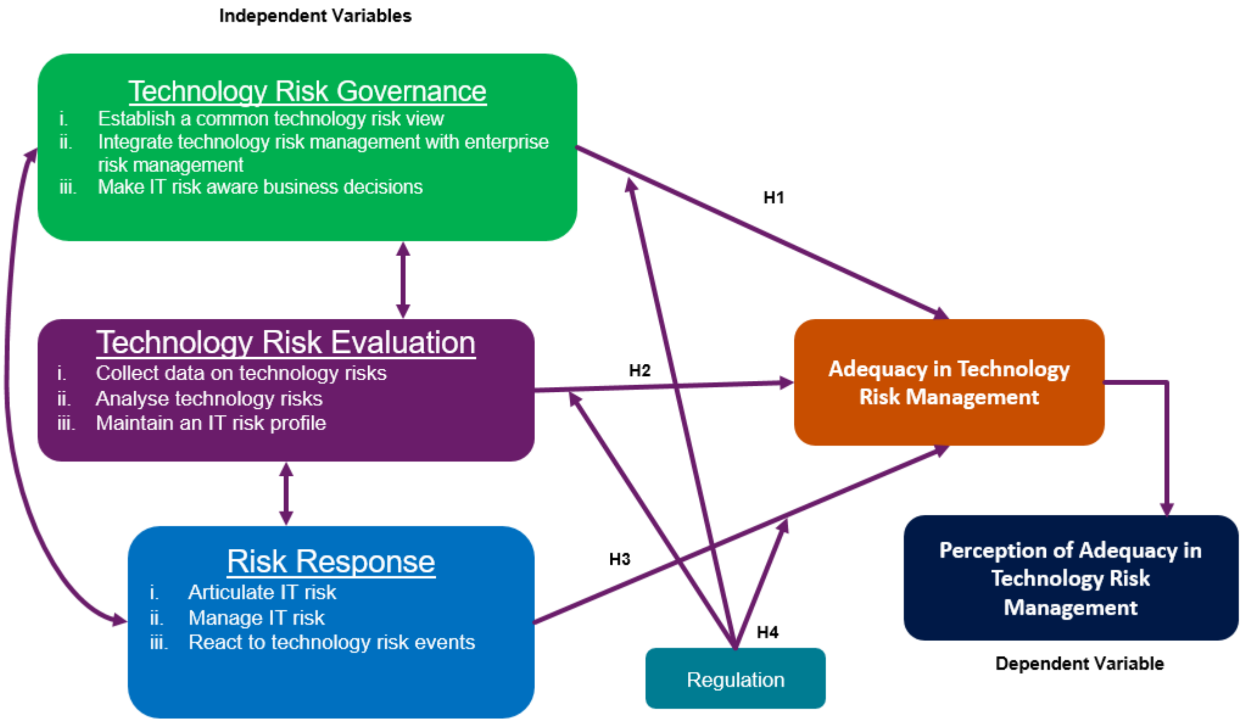

Independent Variables
Technology Risk Governance
i. Establish a common technology risk view
ii. Integrate technology risk management with enterprise risk management
iii. Make IT risk aware business decisions
Technology Risk Evaluation
i. Collect data on technology risks
ii. Analyse technology risks
iii. Maintain an IT risk profile
Risk Response
i. Articulate IT risk
ii. Manage IT risk
iii. React to technology risk events
H1
H2
H3
H4
Regulation
Adequacy in Technology Risk Management
Perception of Adequacy in Technology Risk Management
Dependent Variable

Figure 2: Conceptual framework

Hypothesis 1 – IT risk governance has a significant influence on the adequacy of technology risk management.

Hypothesis 2 – IT risk evaluation has an influence on the adequacy of technology risk management.

Hypothesis 3 – IT risk response mechanisms have an effect on the adequacy of technology risk management.

Hypothesis 4 – Whether a firm is regulated or not has an effect on its adequacy of technology risk management

CHAPTER THREE

RESEARCH METHODOLOGY

This chapter provides information into how research was conducted. It provides a look into the design, data collection methods and the analysis adopted to examine technology risks associated with mobile money lending.

3.1 Research Design

A research design gives an understanding into the structure through which the study was conducted, it contains information on the collection and analysis of key data relevant to the subject of study (Kombo & Tromp, 2006). In particular and of interest to this study, the deduction research approach that involves the development of hypothesis, designing of a research strategy and the detailed step-by-step investigation of relationships (Saunders, Lewis, & Thornhill, 2012) was applied.

This study also used the descriptive approach in aligning the requirements identified by the conceptual framework. To realise this, the study adopted surveys achieved through questionnaires keen to understand technology risk management practices among digital lenders.

3.2 Target Population Data Source

Kenya comprises of 43 banks, all regulated by the Central Bank of Kenya (Central Bank of Kenya, 2017) with the top 8 accounting for 95% of the market share of loan accounts. Five of the eight banks have offer mobile money lending primarily through M-PESA (Safaricom M-PESA, 2019).

The subjects of this study were drawn from all the 5 banks as shown in Table1, this accounted for a 93.7% market share (Central Bank of Kenya, 2017). The criteria for selection of the unregulated lenders included market presence, volume lending and market brand recognition.

Table 1: Sampled Mobile Lenders

	Bank	Number of Loan Accounts (in Millions)	% of the Market
1	KCB Bank Kenya Ltd	1.263	17.70%
2	Co - operative Bank of Kenya Ltd	0.62	8.70%
3	Equity Bank Kenya Ltd	0.67	9.40%
4	Standard Chartered Bank (K) Ltd	0.05	0.70%
5	Diamond Trust Bank	0.015	0.20%
6	Barclays Bank of Kenya Ltd	0.222	3.10%
7	Commercial Bank of Africa	3.92	54.80%
8	Stanbic Bank Kenya Ltd	0.032	0.40%
	Total	**6.792**	**94.90%**

3.3 Sampling Frame and Technique

Purposive sampling was employed in this research as it enables a researcher to select information that is relevant and rich in content to the issues under study (Kombo & Tromp, 2006). In this case, purposive sampling is applied to only the institutions that are offering mobile money lending.

A sample size of 30 and above was deemed acceptable (Oates, 2006). The research required input from respondents at various levels involved in the technology risk management and digital lending process e.g. top management, supervisors and junior staff; as well employees in different areas of specialization e.g. technology, credit, finance, systems audit, financial audit. From each of these stratums, simple random sampling was used to select respondents from whom information was obtained.

Table 2: Sampling Frame for Questionnaires

Department	Function	Sample
Technology	Systems Design, Maintenance and Development	10
Audit	Systems Audit	10
Credit	Lending Management	10
Risk	Risk Management	10
Information Security	Cyber and information security management	10

3.4 Sources and Collection of Data

There can be two types of data sources for a researcher depending on study requirements and goals, these are primary and secondary data. (Kombo & Tromp, 2006).

Primary data would consists of data collected by researchers for identified research purposes while secondary data is information created by other scholars or organizational entities and made available (Saunders, Lewis, & Thornhill, 2012). The researcher used primary data that was obtained through questionnaires.

Questionnaires were constructed based on the research objectives and the framework requirements on the domains and processes. Permission to carry out the research was obtained in advance through a letter from the university. The data was collected through questionnaires as it provided an opportunity for anonymity. The questionnaire had both open ended and closed ended items.

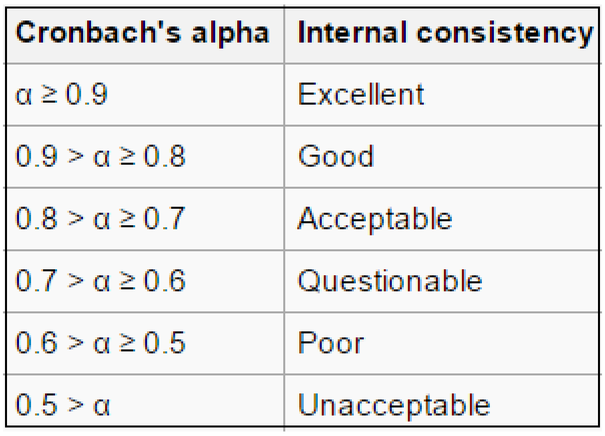
3.4.1 Validity and Reliability Testing of Questionnaire

Reliability can be defined as the error in measurement and is useful in indicating the precision of research instruments prior to deployment. (Esposito, 2004). To test for reliability, responses from selected institutions were subjected to the Cronbach's Alpha Coefficient test. Cronbach's Alpha is a commonly used by researchers to demonstrate that instruments are fit for use (Taber, 2018)

The formula used for the measurement is as below:

$$\text{Cronbach's } Alpha = \frac{Number\ of\ Items * Average\ Covariance\ Between\ Item\ Pairs}{Average\ Variance + (Number\ of\ Items - 1) * Average\ Covariance\ in\ Item\ Pairs}$$

The result from the reliability assessment was a score of 0.78. The procedure used to apply feedback from the reliability testing by the researcher was the revision of the questionnaires where applicable.



Cronbach's alpha	Internal consistency
α ≥ 0.9	Excellent
0.9 > α ≥ 0.8	Good
0.8 > α ≥ 0.7	Acceptable
0.7 > α ≥ 0.6	Questionable
0.6 > α ≥ 0.5	Poor
0.5 > α	Unacceptable

Figure 3: Interpretation of Cronbach's Alpha

Validity is the accuracy of inferences based on research results (Mugenda, 2008).

To establish the validity of the questionnaire, three experts were provided with the questionnaire. One expert was an information systems auditor, another was a financial analyst while the last one was a credit rating professional. Each of the experts scored items each item on a scale and gave recommendations. The recommendations helped to improve the questionnaire wording and placement.

The content validity index (CVI) was calculated as:

$$\text{Content Validity Index} = \frac{Agreed\ Items\ by\ Experts\ as\ Suitable\ and\ Valid}{Total\ Number\ of\ Items}$$

Table 3: Content Validity Index Measurement

	Relevant	**Not Relevant**	**Total**
Information Systems Auditor (Expert 1)	30	3	33
Credit Risk Analyst (Expert 2)	28	5	33
Financial Analyst (Expert 3)	31	2	33
Total	**89**	**10**	**99**

The CVI value obtained of 0.8989 enabled the questionnaire to pass the validity test. A pilot test was conducted after establishing the reliability and validity.

3.4.2 Pilot Testing

The researcher conducted a pilot testing of the questionnaire in two institutions after obtaining a letter from the university. The main reason why piloting the questionnaires was important was to enable the researcher ensure that measurements are of acceptable reliability and validity.

3.5 Research Method

Research methods are classified into two; qualitative and quantitative methods (Orodho, 2009).

Qualitative methods involve the analysis of non-numerical data, they are subjective in nature and descriptive (Creswell, 2014). The quantitative methods are substantive and are based on objective measurements that involved statistical analysis of research data.

This research applied the quantitative method by following the approach of most research studies conducted. This helped the analysis of the strategies applied in strengthening technology risks management in mobile money lending.

3.5.1 Data Analysis

The data that was collected was grouped into various categories according to the RiskIT framework. These categories are: IT risk governance, evaluation and response. The data analysis methods employed gave a result with a highlight of the focus areas and current landscape in technology risks for mobile money lenders in Kenya.

The analysis has been performed in the R Statistical Computing Language (https://www.r-project.org/) and SPSS (https://www.ibm.com/analytics/spss-statistics-software)

Using SPSS, quantitative data was analysed using descriptive statistics; tables, percentages and frequency counts to describe distributions. Using R, a linear regression model was built to test hypothesis and relationships between the dependent and the independent variables.

CHAPTER FOUR

RESULTS AND DISCUSSION

This chapter presents the results of the study and the interpretation of the findings in context of the research objectives. The results are presented using tables, chart and graphs for ease of understanding and interpretation.

4.1.1 Rate of Completion of Questionnaires by Respondents

A tested and approved questionnaire was provided to respondents on an online platform and below is the status of the completed and returned responses.

Table 4: Rate of Completion of Questionnaire

Section	**Department**	**Target**	**Response**	**Return**
Regulated Digital Lenders (Banks) and Unregulated Mobile Lenders	Technology	10	10	100%
	Audit	10	10	100%
	Credit	10	10	100%
	Risk	10	10	100%
	Information Security	10	10	100%
Total		**50**	**50**	**100%**

4.1.2 Demographic Analysis

Tier 1 banking institutions accounted for 50% of the respondents, 40% of the respondents were from unregulated mobile lenders while 10% of the population was pooled from an MFI. The respondents also belonged to specific departments that contribute to the process of mobile money lending in their institutions. These are Technology (20%), Information Systems Audit (20%), Credit (20%), Risk Management (20%) and Information Security (20%).

Table 5: Category of Mobile Lending Institution

		Frequency	Percent	Cumulative Percent
Valid	Mobile Lender - Over 24 Months in Existence	20	40.0	40.0
	Tier 1 Bank	25	50.0	90.0
	Tier 3 Bank	5	10.0	100.0
	Total	**50**	**100.0**	

Source: Research Data, 2019

4.2 Technology Risk Governance Results

Each research item was linked to the framework of study. The governance domain of the RiskIT framework helps organizations ensure that technology risk processes are engrained in the firm-wide activities.

4.2.1 Establish and Maintain a Common IT Risk View

The research was interested in understanding key aspects of risk governance according to the RiskIT ISACA framework. One such aspects is establishing a common IT risk view across the mobile lending business line.

i. **RG1.1 Perform enterprise IT risk assessment**

Respondents were requested to provide feedback if they have had an IT risk assessment within a financial year. The results show that all the regulated entities (100%) have performed an IT risk assessment while a majority (75%) of the unregulated mobile lenders had not.

In the last financial year, has your organization had an IT risk assessment or have you been made aware of one? *

	Regulation		Total
	Regulated	Unregulated	
Yes	100.0%	25.0%	70.0%
No		75.0%	30.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019.

From the above results, it is evident that 75% of unregulated mobile lenders do not have opportunities to help business managers understand IT risk in the context of activities that are pertinent to daily responsibilities.

ii. RG1.2 and RG1.3 Propose and Approve IT risk tolerance thresholds

Respondents were requested to provide feedback if they have had approved documentation on the amount of IT related risks the organization could take. The results show that some of the regulated entities (83.3%) had approved documentation on risk thresholds while 100% of the unregulated entities had no such document.

Does your mobile lending business have an approved documentation of the amount of IT related risk it can take?

	Regulation		Total
	Regulated	Unregulated	
Yes	83.3%		50.0%
No	16.7%	100.0%	50.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019.

iii. RG1.4 Align IT risk policy

Respondents were requested to provide feedback if they had approved IT risk policies. All the regulated lenders had an approved IT risk policy while close to half of the respondents from unregulated environments (45%) informed that their organizations did not have an approved IT Risk Policy.

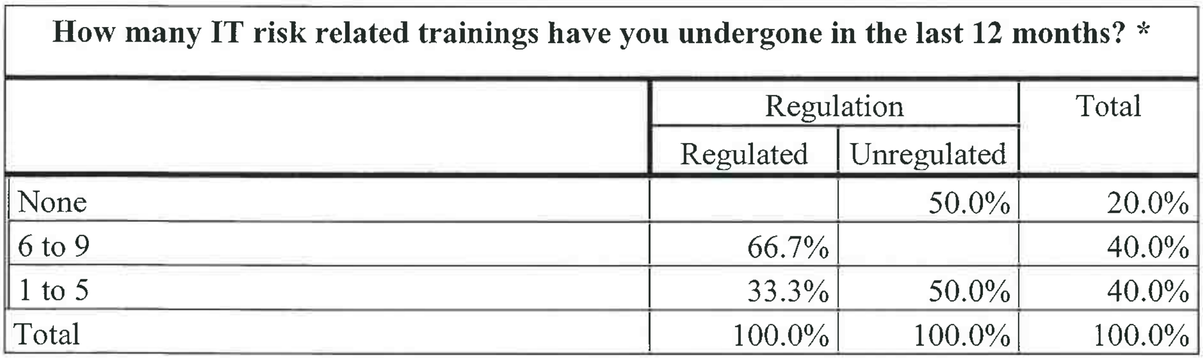
Does your organization have an approved IT Risk Policy?

	Regulation		Total
	Regulated	Unregulated	
Yes	100.0%	55.0%	82.0%
No		45.0%	18.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019.

iv. RG1.5 Promote IT risk-aware culture

Respondents were requested to provide feedback if they had undergone an IT risk related training within the last 12 months. Regulated entities had taken trainings while 50% of the respondents from unregulated entities had not undertaken any IT risk related trainings.



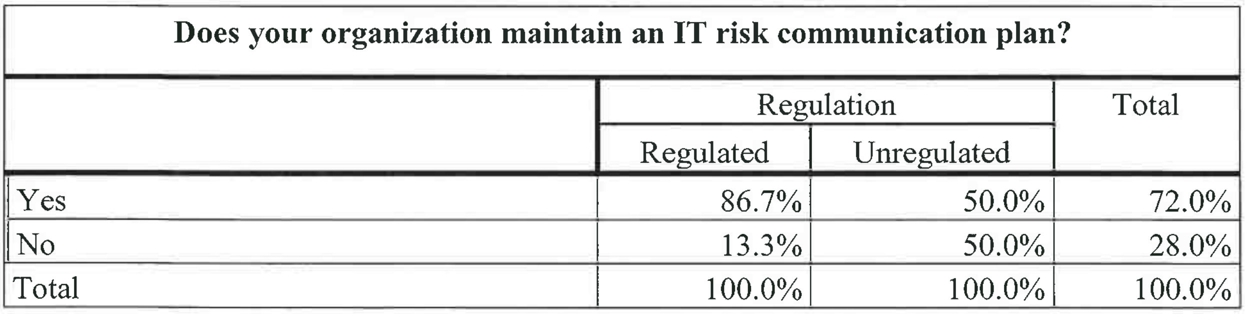
How many IT risk related trainings have you undergone in the last 12 months? *

	Regulation		Total
	Regulated	Unregulated	
None		50.0%	20.0%
6 to 9	66.7%		40.0%
1 to 5	33.3%	50.0%	40.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019.

v. RG1.6 Encourage effective communication of IT risk

Respondents were requested to provide feedback if their organizations maintained an IT Risk Communication Plan. A majority of regulated entities (86.7%) had an IT risk communication plan while for unregulated entities, half of the respondents (50%) gave feedback that their entities did not have an IT risk communication plan.



Does your organization maintain an IT risk communication plan?

	Regulation		Total
	Regulated	Unregulated	
Yes	86.7%	50.0%	72.0%
No	13.3%	50.0%	28.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019.

4.2.2 Integrate Technology Risk Management with Enterprise Risk

The research was interested in assessing feedback on the integration of technology risk management with enterprise wide risk management. According to the RiskIT framework, this can be broken down into a number of elements.

i. RG2.1 Establish and maintain accountability for IT risk management

Respondents were requested to provide feedback on who was responsible and accountable for IT risk management within their organizations.

A majority of respondents in banks (63.3%) provided feedback that it is the responsibility of every individual within the organization to manage IT risk while for unregulated entities, 70% of the respondents felt that the responsibility belongs to the Board of Directors.

Who is responsible and accountable in IT risk Management in your organization?

	Regulation		Total
	Regulated	Unregulated	
Risk Management	13.3%	5.0%	10.0%
IT	13.3%		8.0%
Everyone Across the Enterprise	63.3%	10.0%	42.0%
CEO		15.0%	6.0%
Board of Directors	10.0%	70.0%	34.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019.

ii. RG2.2 and RG2.3 Co-ordinate and Adapt IT risk strategy and business risk strategy

Respondents were requested to provide feedback on who was responsible and accountable for IT risk management within their organizations.

A majority of respondents from regulated entities (86.7%) consider that their IT risk strategies are aligned to business risk initiatives while 75% of the respondents in unregulated mobile lenders gave feedback that their IT risk strategy was not aligned to business.

I consider the organization's IT risk strategy aligned to the business strategy.

	Regulation		Total
	Regulated	Unregulated	
Neither Agree or Disagree	10.0%	5.0%	8.0%
Disagree	3.3%	75.0%	32.0%
Agree	86.7%	20.0%	60.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019.

iii. RG2.4 Provide adequate resources for IT risk management

Respondents were requested to provide feedback if they had faced any resource constraints in their execution of IT risk management.

Overall, regulated (90%) and all unregulated entities gave feedback that in the execution of their duties related to IT risk management, they had faced resource constraints.

Have you faced resource constraints in your execution of IT risk management in the last financial year?

	Regulation		Total
	Regulated	Unregulated	
Yes	90.0%	100.0%	94.0%
No	10.0%		6.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019.

iv. RG2.5 Provide independent assurance over IT risk management

Respondents were requested to provide feedback if their organization had performed an external IT audit. Overall, a majority of the regulated (83%) had performed an external IT audit within the last financial year. None of the unregulated entities had done the same.

Have you performed an external audit of IT or IT risk in the last financial year?

	Regulation		Total
	Regulated	Unregulated	
Yes	83.3%		50.0%
No	16.7%	100.0%	50.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019

4.2.3 Making IT Risk Aware Business Decisions

The study was interested in assessing feedback on whether the making of business decisions was cognizant of IT risks. This is important as it ensures that enterprise decisions consider the all possible technology risk scenarios.

According to the RiskIT framework, this can be broken down into a number of elements.

i. RG3.1 Gain management buy-in for the IT risk analysis approach

Respondents were requested to provide feedback if within their organizations, management had a proactive role in encouraging active involvement in IT risk management.

Overall, a majority of the regulated entities (83%) had close management involvement in encouraging IT risk management while all of the unregulated entities where unsure.

Does your management push for your proactive involvement in management of IT Risk?

	Regulation		Total
	Regulated	Unregulated	
Yes	83.3%		50.0%
Not Sure		100.0%	40.0%
No	16.7%		10.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019

ii. RG3.2 Approve IT risk analysis

Respondents were requested to provide feedback if within their organizations they had an IT risk analysis report valid for the current financial year.

Overall, all of the regulated entities (100%) had an IT risk analysis report whole 70% of the unregulated entities did not have a report of IT risk.

Does your organization have an IT risk analysis report valid in the current financial year

	Regulation		Total
	Regulated	Unregulated	
Yes	100.0%	30.0%	72.0%
No		70.0%	28.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019

iii. RG3.3 Embed IT risk considerations in strategic business decision making

Respondents were requested to provide feedback if they agreed that their organization considered IT risk prior to making critical business decisions.

Overall, all of the unregulated entities (100%) could not confirm if their organizations considered IT risk in business decisions while 70% of the regulated entities could confirm that their key business decisions were made with IT risk in mind.

Do you agree that your organization considers IT risk prior to making key business decisions?

	Regulation		Total
	Regulated	Unregulated	
Strongly Agree	10.0%		6.0%
Neither Agree nor Disagree	20.0%	100.0%	52.0%
Agree	70.0%		42.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019

iv. RG3.4 Accept IT risk

Respondents were requested to provide feedback if their mobile lending business documented all IT risk acceptance decisions.

Overall, all of the regulated entities (100%) could confirm that they documented IT risk acceptance decisions while all of the unregulated entities did not.

Does your mobile lending business maintain documentation of IT risk acceptance decisions?

	Regulation		Total
	Regulated	Unregulated	
Yes	100.0%		60.0%
No		100.0%	40.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019

v. RG3.5 Prioritise IT risk response activities

Respondents were requested to provide feedback if their organizations prioritized IT risk response activities.

Overall, all of the regulated entities (100%) could confirm that their entities prioritized IT risk response activities while a majority of respondents from the unregulated entities (80%) could not confirm or disagreed (20%).

Do you agree that your organization prioritizes IT risk response activities? *

	Regulation		Total
	Regulated	Unregulated	
Strongly Agree	33.3%		20.0%
Neither Agree nor Disagree		80.0%	32.0%
Disagree		20.0%	8.0%
Agree	66.7%		40.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019

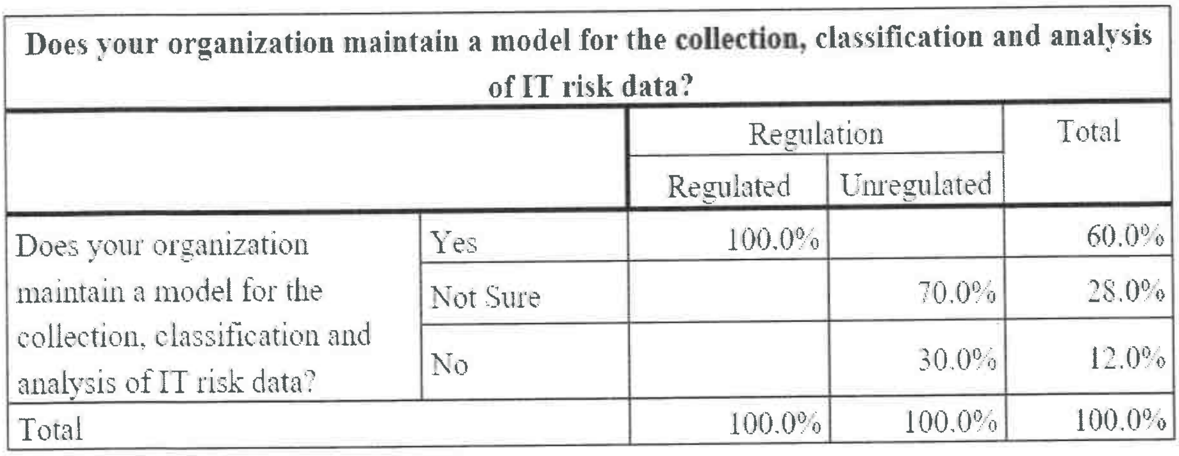
4.3 Technology Risks Evaluation Results and Discussion

Each research item was linked to the framework of study. The results below relate to the risk evaluation domain of the RiskIT framework. The domain is focused on helping entities ensure technology risks are identified, analysed and communicated in terms understood by business.

4.3.1 Data Collection and Classification Model

The study was keen to assess if organizations maintained capabilities for the collection, maintenance and analysis of technology risk data. The model would classify external risk factors that are relevant to IT risk in the context of mobile lending.

70% of the respondents from the unregulated entities were unsure if their organization maintained a model for IT risk data collection. 30% of the respondents from the unregulated entities could confirm that their entities did not maintain a model on IT risk data. All the regulated entities confirmed that data on IT risk was maintained in form of risk logs. These were updated on a continuous basis.



Does your organization maintain a model for the collection, classification and analysis of IT risk data?

		Regulation		Total
		Regulated	Unregulated	
Does your organization maintain a model for the collection, classification and analysis of IT risk data?	Yes	100.0%		60.0%
	Not Sure		70.0%	28.0%
	No		30.0%	12.0%
Total		100.0%	100.0%	100.0%

Source: Research Data, 2019

4.3.2 Analyse IT Risk

The study was interested in understanding how mobile lending entities analysed IT risk. Analysing IT risk involves the continuous documentation of useful data and analytics to support business decisions by taking into account factors of technology risk.

This could be measured in a number of ways according to the RiskIT framework.

i. **RE2.1 Define IT risk analysis scope**

Respondents were requested to provide feedback if their organizations defined their IT risk analysis scope. It is particularly important for entities to decide on the expected investments of time and efforts into risk analysis efforts so as prioritize activities.

Overall, all of the regulated entities could confirm that their entities defined their IT risk response activities while a majority of respondents from the unregulated entities (80%) could not confirm or disagreed (20%).

Do you agree that your organization defines its risk analysis scope

	Regulation		Total
	Regulated	Unregulated	
Strongly Agree	10.0%		6.0%
Neither Agree nor Disagree		80.0%	32.0%
Disagree		20.0%	8.0%
Agree	90.0%		54.0%
Total	**100.0%**	**100.0%**	**100.0%**

Source: Research Data, 2019

ii. RE2.2 Estimate IT risk

Respondents were requested to provide feedback if their organizations estimated IT risk exposure through assessment of likelihood and impact. Overall, all of the regulated entities could confirm that their entities estimated their IT risk exposure while a majority of respondents from the unregulated entities (75%) could not confirm or disagreed (25%).

My organization estimates its risk exposure through assessment of likelihood and impact.

	Regulation		Total
	Regulated	Unregulated	
Neither Agree nor Disagree		75.0%	30.0%
Disagree		25.0%	10.0%
Agree	100.0%		60.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019

iii. RE2.3 Identify risk response options

Respondents were requested to provide feedback if their organizations identified risk response options for each type of risk as per internal policy and business requirements. Overall, all of the regulated entities could confirm that their entities had a clear understanding of the available options on risk response while a majority of respondents from the unregulated entities (70%) could not confirm or disagreed (30%).

My organization has a clear understanding of its range of risk response options

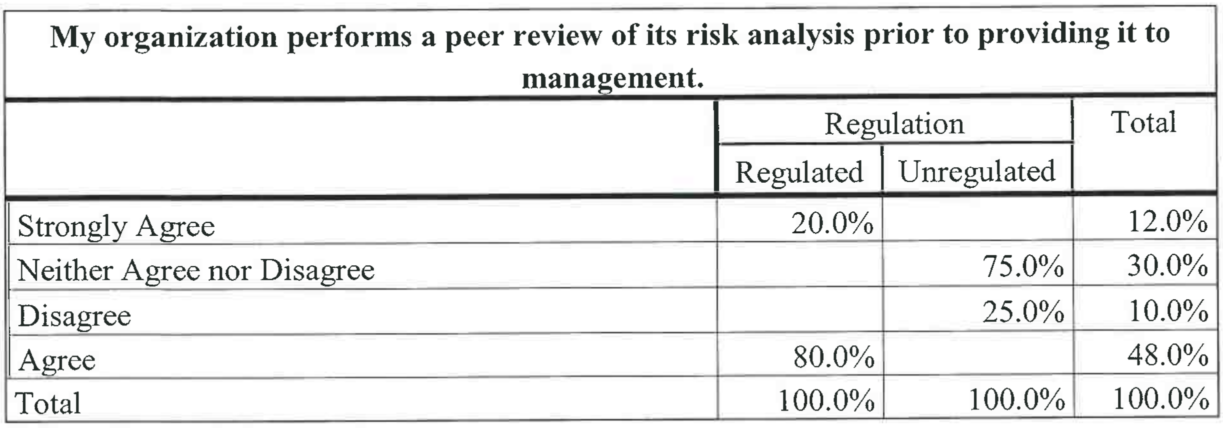
	Regulation		Total
	Regulated	Unregulated	
Strongly Agree	23.3%		14.0%
Neither Agree nor Disagree		70.0%	28.0%
Disagree		30.0%	12.0%
Agree	76.7%		46.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019

iv. RE2.4 Perform a peer review of IT risk analysis

Respondents were requested to provide feedback if their organizations performed peer review of IT risk analysis prior to sharing results with management for decision making.

Overall, all of the regulated entities could confirm that their entities performed peer review activities while a majority of respondents from the unregulated entities (75%) could not confirm or disagreed (25%).



My organization performs a peer review of its risk analysis prior to providing it to management.

	Regulation		Total
	Regulated	Unregulated	
Strongly Agree	20.0%		12.0%
Neither Agree nor Disagree		75.0%	30.0%
Disagree		25.0%	10.0%
Agree	80.0%		48.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019.

4.3.3 Maintaining an IT Risk Profile

The study was interested in knowing how mobile money lenders were able to maintain a risk profile of all possible technology risks that is up-to-date.

i. RE3.1 Map IT resources to business processes

Respondents were requested to provide feedback if their organizations mapped IT resources to key business processes.

Overall, a majority of the regulated entities (83%) could confirm that their entities mapped IT resources to business processes. 80% of respondents from the unregulated entities responded that their organizations had not mapped IT resources to key business processes.

Does your organization have a map of its IT resources to key business processes?

	Regulation		Total
	Regulated	Unregulated	
Yes	83.3%		50.0%
Not Sure		20.0%	8.0%
No	16.7%	80.0%	42.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019.

ii. RE3.2 Determine business criticality of IT resources

Respondents were further requested to provide feedback if their organizations had determined the business criticality of their IT resources.

Overall, all of the regulated entities could confirm that their entities determined how critical IT resources were to business while a majority of respondents from the unregulated entities (75%) could not confirm or disagreed (25%).

My organization determines which IT services and IT infrastructure resources are required to sustain the operation of key services and critical business processes.

	Regulation		Total
	Regulated	Unregulated	
Strongly Agree	20.0%		12.0%
Neither Agree nor Disagree		75.0%	30.0%
Disagree		25.0%	10.0%
Agree	80.0%		48.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019

iii. RE3.3 Understand IT capabilities

Respondents were requested to provide feedback if their organizations had evaluated IT capabilities across the landscape of technology risk. Overall, all of the regulated entities could confirm that their entities had evaluated its IT capabilities in the context of IT risk while all of the respondents from the unregulated entities disagreed (100%).

My organization evaluates its IT process capability, skills and knowledge of people, and IT performance outcomes across the spectrum of IT risk.

	Regulation		Total
	Regulated	Unregulated	
Strongly Agree	20.0%		12.0%
Disagree		100.0%	40.0%
Agree	80.0%		48.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019

iv. RE3.4 Update IT risk scenario components

Respondents were requested to provide feedback if their organizations reviewed the collection of key metadata and attributes on possible technology risk scenarios.

Overall, all of the regulated entities could confirm that their entities had collected IT risk scenario components while 80% of the respondents from the unregulated entities could not confirm and 20% disagreed.

My organization reviews the collection of attributes and values across IT risk scenario components

	Regulation		Total
	Regulated	Unregulated	
Neither Agree nor Disagree		20.0%	8.0%
Disagree		80.0%	32.0%
Agree	100.0%		60.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019.

v. RE3.5 Maintain the IT risk register and IT risk map

Respondents were requested to provide feedback if their organizations maintained tools like register and risk maps to enable them capture and monitor IT risks.

Overall, all of the regulated entities could confirm that their entities had a risk register or risk map for IT while 20% of the respondents from the unregulated entities could not confirm and 80% disagreed.

My organization captures its IT risk profile within tools such as an risk registers and maps

	Regulation		Total
	Regulated	Unregulated	
Strongly Agree	26.7%		16.0%
Neither Agree nor Disagree		20.0%	8.0%
Disagree		80.0%	32.0%
Agree	73.3%		44.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019.

vi. RE3.6 Develop IT risk indicators

Respondents were requested to provide feedback if their organizations developed technology risk indicators for events that can significantly impact the operational capacity of business. Overall, 93.3% of the regulated entities could confirm that their entities had a designed metrics or indicators for IT risk event assessment while 80% of the respondents from the unregulated entities could not confirm or disagreed (20%).

My organization designs metrics or indicators that can point to IT-related events and incidents that can significantly impact the business.

	Regulation		Total
	Regulated	Unregulated	
Strongly Agree	13.3%		8.0%
Neither Agree nor Disagree	6.7%	80.0%	36.0%
Disagree		20.0%	8.0%
Agree	80.0%		48.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019.

4.4 Results on Response to Digital Lending Risks and Discussion

Each research item was linked to the framework of study. The results below relate to the risk response domain of the RiskIT framework. The domain focusses on helping organizations address opportunities and events within a framework that is cost conscious with priorities biased to business.

4.4.1 Articulation of IT Risk

The study was interested in knowing how mobile money lenders ensured that information on the technology risk exposures is made available for appropriate response.

i. RR1.1 Communicate IT risk analysis results

Respondents were requested to provide feedback if their organizations reported IT risk analysis in terms that are understood by business.

Overall, 96.6% of the regulated entities could confirm that their entities had reported IT risk analysis results with clarity to business decision makers. 80% of the respondents from the unregulated entities could not confirm that their results where applicable were communicated in terms and formats useful to business decision makers, 15% of the respondents were able to confirm.

My organization reports its IT risk analysis results in business terms

	Regulation		Total
	Regulated	Unregulated	
Strongly Agree	33.3%		20.0%
Neither Agree nor Disagree	3.3%	80.0%	34.0%
Disagree		5.0%	2.0%
Agree	63.3%	15.0%	44.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019.

ii. RR1.2 Report IT risk management activities and state of compliance

Respondents were requested to provide feedback if they considered IT risk analysis reporting to be strategic and efficient. Overall, all of the regulated entities could confirm that their entities' reporting of IT risk analysis results was strategic and efficient. 80% of the respondents from the unregulated entities could not confirm that their reporting was strategic or efficient.

I consider reporting on IT risk issues and status in my organization to be strategic and efficient.

	Regulation		Total
	Regulated	Unregulated	
Neither Agree nor Disagree		80.0%	32.0%
Disagree		10.0%	4.0%
Agree	100.0%	10.0%	64.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019.

iii. RR1.3 Interpret independent IT assessment findings

Respondents were requested to provide feedback if their organizations could independently interpret review findings of objective third parties such as internal audit, quality assurance, external audit, among others

Overall, 96.6% of the respondents from regulated entities could confirm that they were able to review the results from independent IT assurance. 90% of the respondents from the unregulated entities could not confirm.

My organization is able to review the results and specific findings of from third party independent IT assurance professionals.

	Regulation		Total
	Regulated	Unregulated	
Strongly Agree	13.3%		8.0%
Neither Agree nor Disagree	3.3%	90.0%	38.0%
Agree	83.3%	10.0%	54.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019.

iv. RR1.4 Identify IT-related opportunities

Respondents were requested to provide feedback if they were able to opportunities for technology enabled lending that could help business accept greater technology risk and ensure accelerated growth and higher profitability.

Overall, all of the respondents from regulated entities could confirm that they were able to identify IT related opportunities. 95% of the respondents from the unregulated entities could also confirm that they could identify business impacting IT-related opportunities.

My organization is able to identify IT-related opportunities that could enable mobile money lending to accept greater risk and enhance growth and return.

	Regulation		Total
	Regulated	Unregulated	
Strongly Agree	13.3%		8.0%
Disagree		5.0%	2.0%
Agree	86.7%	95.0%	90.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019

4.4.2 Managing IT Risk

The study sought to understand how mobile money lending institutions ensure that measures for technology risk response are centralized and collectively managed.

i. RR2.1 Inventory controls

Respondents were requested to provide feedback if their organization had put in place controls to manage risk.

All the respondents from the regulated entities could confirm at they had an inventory of controls while 95% of the respondents from the unregulated lenders were able to confirm that their organization had put in place across risk focus areas, controls to manage technology risk.

My organization has put in place across risk focus areas, an inventory of controls to manage risk and enable risk to be taken in line with risk appetite and tolerance.

	Regulation		Total
	Regulated	Unregulated	
Strongly Agree	13.3%		8.0%
Disagree		5.0%	2.0%
Agree	86.7%	95.0%	90.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019

ii. RR2.2 Monitor operational alignment with risk tolerance thresholds

Respondents were requested to provide feedback if they ensured that the mobile lending business line accepted accountability for operating within its environment. It was also important to understand if monitoring tools were embedded into key operating processes. 90% the respondents from both the regulated entities and unregulated entities could confirm that accountability and monitoring were part of business line activities.

My organization ensures that the mobile lending business line accepts accountability for operating within its individual environment

	Regulation		Total
	Regulated	Unregulated	
Strongly Agree	10.0%		6.0%
Neither Agree nor Disagree		5.0%	2.0%
Disagree		5.0%	2.0%
Agree	90.0%	90.0%	90.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019

iii. RR2.3 Respond to discovered risk exposure and opportunity

To understand how mobile lending organizations were responding to discovered risk exposure and opportunity, respondents were requested to provide feedback if their organizations held evaluation discussions regarding the value of new or existing risk safeguards to overall business initiatives. All of the respondents from the regulated entities (100%) could confirm while 80% of the respondents from the unregulated entities could not confirm.

My organization holds cost/benefit discussions regarding the contribution of new or existing controls towards operating within IT risk tolerance

	Regulation		Total
	Regulated	Unregulated	
Strongly Agree	16.7%		10.0%
Neither Agree nor Disagree		65.0%	26.0%
Disagree		15.0%	6.0%
Agree	83.3%	20.0%	58.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019

iv. RR2.4 Implement controls

Respondents were requested to provide feedback if their organization takes appropriate steps in control implementation. All of the respondents from the regulated entities (100%) could confirm while 85% of the respondents from the unregulated entities could confirm that their organizations took appropriate steps to ensure that control development met the required standards and objectives.

Where required, my organization takes appropriate steps to ensure the effective deployment of new controls and adjustments to existing controls.

	Regulation		Total
	Regulated	Unregulated	
Neither Agree nor Disagree		10.0%	4.0%
Disagree		5.0%	2.0%
Agree	100.0%	85.0%	94.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019.

v. **RR2.5 Report IT risk action plan progress**

Respondents were requested to provide feedback if their organizations monitors technology risk action plans. All of the respondents from the regulated entities (100%) could confirm that their organizations monitored IT risk action plans while 65% of the respondents from the unregulated entities could not confirm the same.

My organization monitors IT risk action plans at all levels to ensure the effectiveness of required actions and determine whether acceptance of residual risk was obtained.

	Regulation		Total
	Regulated	Unregulated	
Strongly Agree	30.0%		18.0%
Neither Agree nor Disagree		65.0%	26.0%
Disagree		10.0%	4.0%
Agree	70.0%	25.0%	52.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019.

4.4.3 Reaction to IT Risk Events

The research sought to understand how mobile money lending institutions ensure that measures for managing technology opportunities and risks are activated in a timely manner.

i. **RR3.1 Maintain incident response plans**

Respondents were requested to provide feedback if their organizations prepared for the materialisation of IT threats. 96.7% of the respondents from regulated environments confirmed while 85% of the respondents from unregulated environments were also able to confirm that their organizations maintained incident response plans. Overall, across all entities, presence of incident response planning was at 100%.

My organization prepares for any materialisation of threats through plans that illustrate the specific measures to take.

	Regulation		Total
	Regulated	Unregulated	
Neither Agree nor Disagree	3.3%	15.0%	8.0%
Agree	96.7%	85.0%	92.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019.

ii. RR3.2 Monitor IT risk

Respondents were requested to provide feedback if their organizations monitored IT risk on a continuous basis. 83.3% of the respondents from regulated environments confirmed that they monitored IT risk while none of the respondents from unregulated environments could confirm if their organization monitored their IT risk environment.

Does your organization monitor its IT risk environment?

		Regulation		Total
		Regulated	Unregulated	
Does your organization monitor its IT risk environment?	Yes	83.3%		50.0%
	Not Sure		100.0%	40.0%
	No	16.7%		10.0%
Total		100.0%	100.0%	100.0%

Source: Research Data, 2019.

iii. RR3.3 Initiate incident response

Does your organization have an incident response plan?

		Regulation		Total
		Regulated	Unregulated	
Does your organization have an incident response plan?	Yes	100.0%	100.0%	100.0%
Total		100.0%	100.0%	100.0%

Source: Research Data, 2019.

While all respondents highlighted that their entities had incident response plans, the adequacy of the incident response documents would be a useful area of further study. According to research, organized incident response requires defined and repeatable processes. Of critical importance to the process if the ability of institutions to learn from such events. A majority of the information security incidents would put in the jeopardy the confidentiality and integrity of critical systems and data (Ruefle, et al., 2014).

iv. RR3.4 Communicate lessons learned from risk events

Respondents were requested to provide feedback if their organizations examined past adverse events/losses and missed opportunities in order to learn from the events. 83.3% of the respondents from regulated environments confirmed that lessons were communicated while all of the respondents from the unregulated could confirm the same.

My organization examines past adverse events/losses and missed opportunities in order to learn from the events

	Regulation		Total
	Regulated	Unregulated	
Strongly Agree	3.3%		2.0%
Disagree	16.7%		10.0%
Agree	80.0%	100.0%	88.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019.

4.5 DISCUSSION OF RESULTS

4.5.1 Analysis of IT Risk Management Adequacy

The RiskIT framework provides for an assessment of maturity for each of the domain. The assessment was applied in context of the breakdown below.

Table 6: Interpretation of Scoring Criteria

Rating	Range	Interpretation of Scoring Criteria
High	0 - 1	Weaknesses in technology risk management may result in high-risk exposure to the mobile lending institution. All areas under the framework should be reviewed and addressed immediately.
Medium	2 – 3	Any weakness in technology risk management within mobile money lending may result in medium-risk exposure. All areas under the RiskIT framework should be addressed as soon as possible.
Low	4 – 5	Any weakness in technology risk management may result in low-risk exposure and may be addressed in due time. These weaknesses cannot result in compromise of whole/ part of the IT system on their own.

Source: ISACA, 2009

4.5.2 Analysis of Adequacy in Risk Governance

The RiskIT framework by ISACA provides for the following assessment model:

Table 7: Risk Governance Maturity Model

Assessment	Risk Governance Domain
0 – Non Existent	The enterprise does not recognise the need to consider the business impact from IT risk. Decisions involving IT risk taking lack credible information. There is no awareness of external requirements for IT risk management and integration with enterprise risk management.
1 – Initial	There is an emerging understanding that IT risk is important and needs to be managed, but it is viewed as a technical issue and the business primarily considers the downside of IT risk.
2 - Repeatable	There is an awareness of the need to actively manage IT risk, but the focus is on technical compliance with no anticipation of value added. There are emerging leaders for IT risk management within silos who assume responsibility and are usually held accountable, even if this is not formally agreed.
3 – Defined	IT risk management is viewed as a business issue, and both the downside and upside of IT risk are recognised.
4 - Managed	IT risk management is viewed as a business enabler, and both the downside and upside of IT risk are understood
5 – Optimised	Senior executives make a point of considering all aspects of IT risk in their decisions. The IT risk leader is considered a trusted advisor during design, implementation and steady-state operations.

Source: ISACA, 2009

Table 8: Risk Governance Activity Scoring

Domain Activity	Regulated	Unregulated
RG1.1 Perform enterprise IT risk assessment	5.000	1.250
RG1.2 Propose IT risk tolerance thresholds	4.167	-
RG1.3 Approve IT risk tolerance	5.000	2.750
RG1.5 Promote IT risk-aware culture	3.667	1.500
RG1.6 Encourage effective communication of IT risk	4.333	2.500
RG2.2 Co-ordinate IT risk strategy and business risk strategy	2.700	0.650
RG2.4 Provide adequate resources for IT risk management	4.500	5.000
RG2.5 Provide independent assurance over IT risk management	4.167	-
RG3.1 Gain management buy-in for the IT risk analysis	4.167	1.000
RG3.2 Approve IT risk analysis	5.000	1.500
RG3.3 Embed IT risk considerations in strategic decisions	2.700	1.000
RG3.4 Accept IT risk	5.000	-
RG3.5 Prioritise IT risk response activities	3.333	0.800
Average Score	**4.133**	**1.381**
Rating	**Low Risk**	**High Risk**

Source: Research Data, 2019

Based on a score of 1 to 5, entities were scored for each of the domain activities based on their answers to different aspects of technology risk governance.

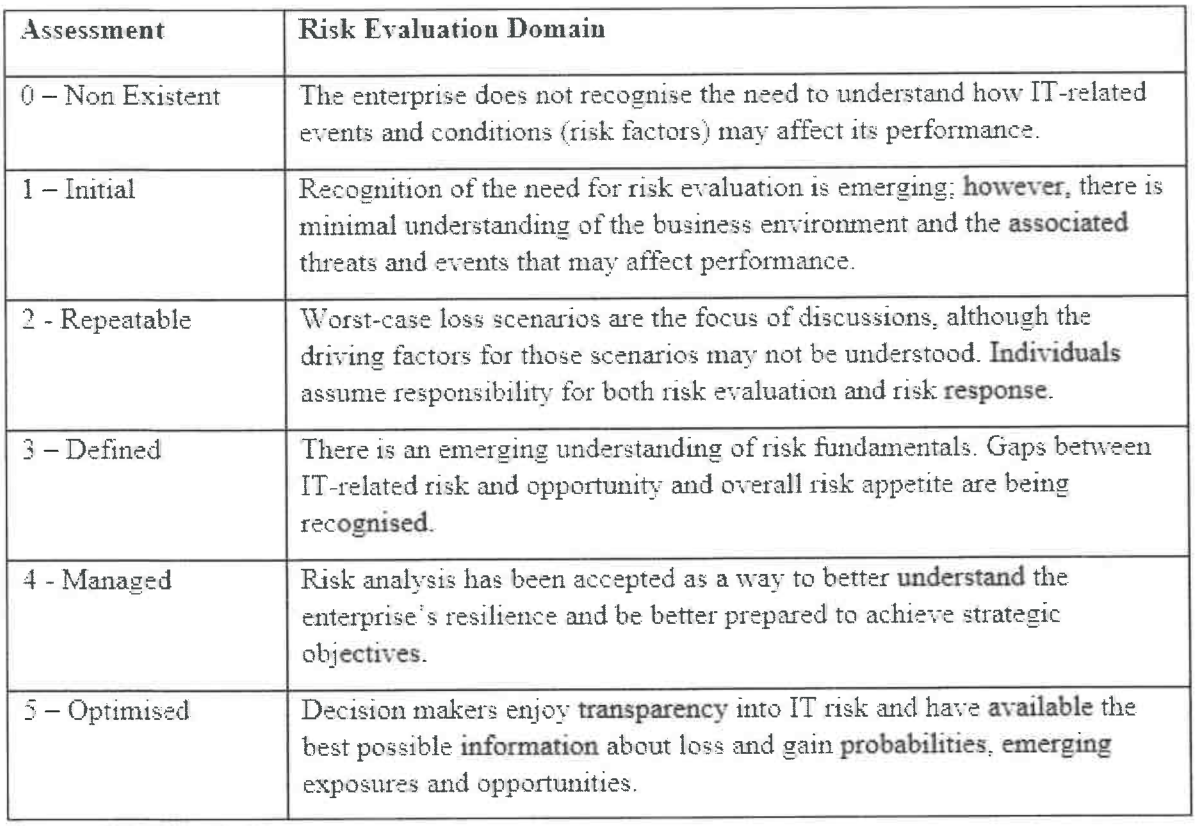
Based on this score, it can be derived that regulated entities that provide mobile lending have an IT risk governance maturity level that is robust and enables business growth. The top down approach is critical to a strengthened IT risk governance structure.

For unregulated entities, there is evidence of weaknesses technology risk governance and accountability. This disadvantages the unregulated lenders as IT risks could materialize through exploitation of areas of weaknesses such as resource and capacity limitations, lack of IT risk policies and misalignment of organizational risk management objectives.

4.5.3 Analysis of Adequacy in Risk Evaluation

The RiskIT framework by ISACA provides for the following assessment model:

Table 9: Risk Evaluation Maturity Model

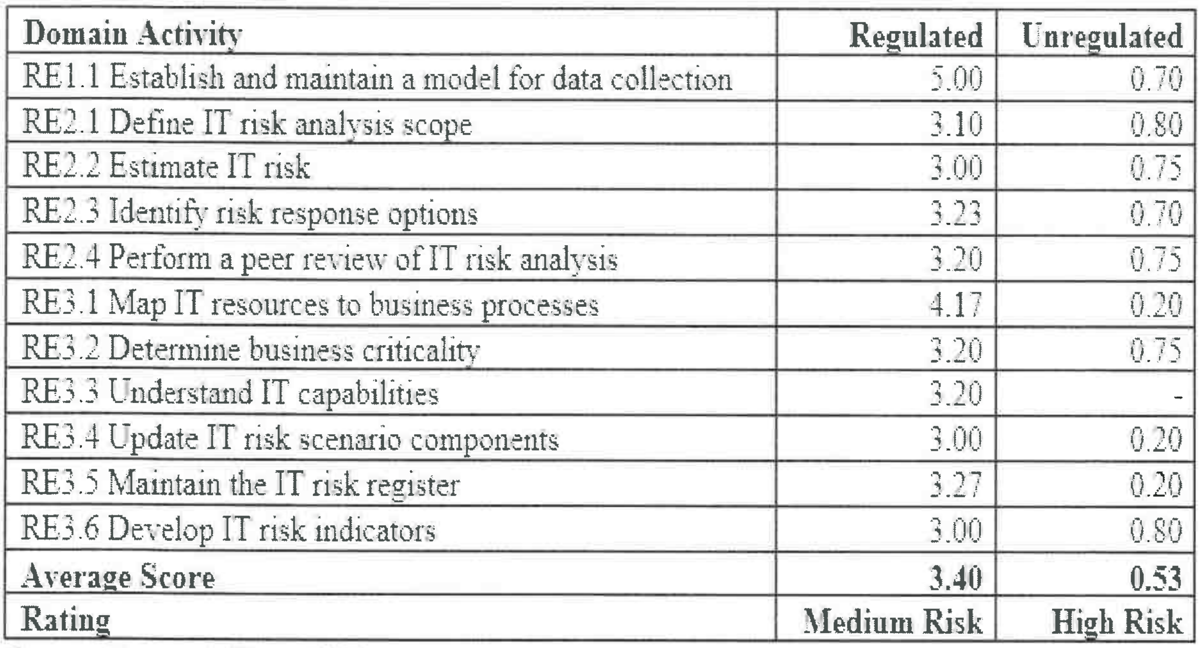


Assessment	Risk Evaluation Domain
0 – Non Existent	The enterprise does not recognise the need to understand how IT-related events and conditions (risk factors) may affect its performance.
1 – Initial	Recognition of the need for risk evaluation is emerging; however, there is minimal understanding of the business environment and the associated threats and events that may affect performance.
2 - Repeatable	Worst-case loss scenarios are the focus of discussions, although the driving factors for those scenarios may not be understood. Individuals assume responsibility for both risk evaluation and risk response.
3 – Defined	There is an emerging understanding of risk fundamentals. Gaps between IT-related risk and opportunity and overall risk appetite are being recognised.
4 - Managed	Risk analysis has been accepted as a way to better understand the enterprise's resilience and be better prepared to achieve strategic objectives.
5 – Optimised	Decision makers enjoy transparency into IT risk and have available the best possible information about loss and gain probabilities, emerging exposures and opportunities.

Source: ISACA, 2009

Based on a score of 1 to 5, entities were scored for each of the domain activities based on their answers to different aspects of technology risk evaluation.

Table 10: Risk Evaluation Activity Scoring



Domain Activity	Regulated	Unregulated
RE1.1 Establish and maintain a model for data collection	5.00	0.70
RE2.1 Define IT risk analysis scope	3.10	0.80
RE2.2 Estimate IT risk	3.00	0.75
RE2.3 Identify risk response options	3.23	0.70
RE2.4 Perform a peer review of IT risk analysis	3.20	0.75
RE3.1 Map IT resources to business processes	4.17	0.20
RE3.2 Determine business criticality	3.20	0.75
RE3.3 Understand IT capabilities	3.20	-
RE3.4 Update IT risk scenario components	3.00	0.20
RE3.5 Maintain the IT risk register	3.27	0.20
RE3.6 Develop IT risk indicators	3.00	0.80
Average Score	**3.40**	**0.53**
Rating	**Medium Risk**	**High Risk**

Source: Research Data, 2019

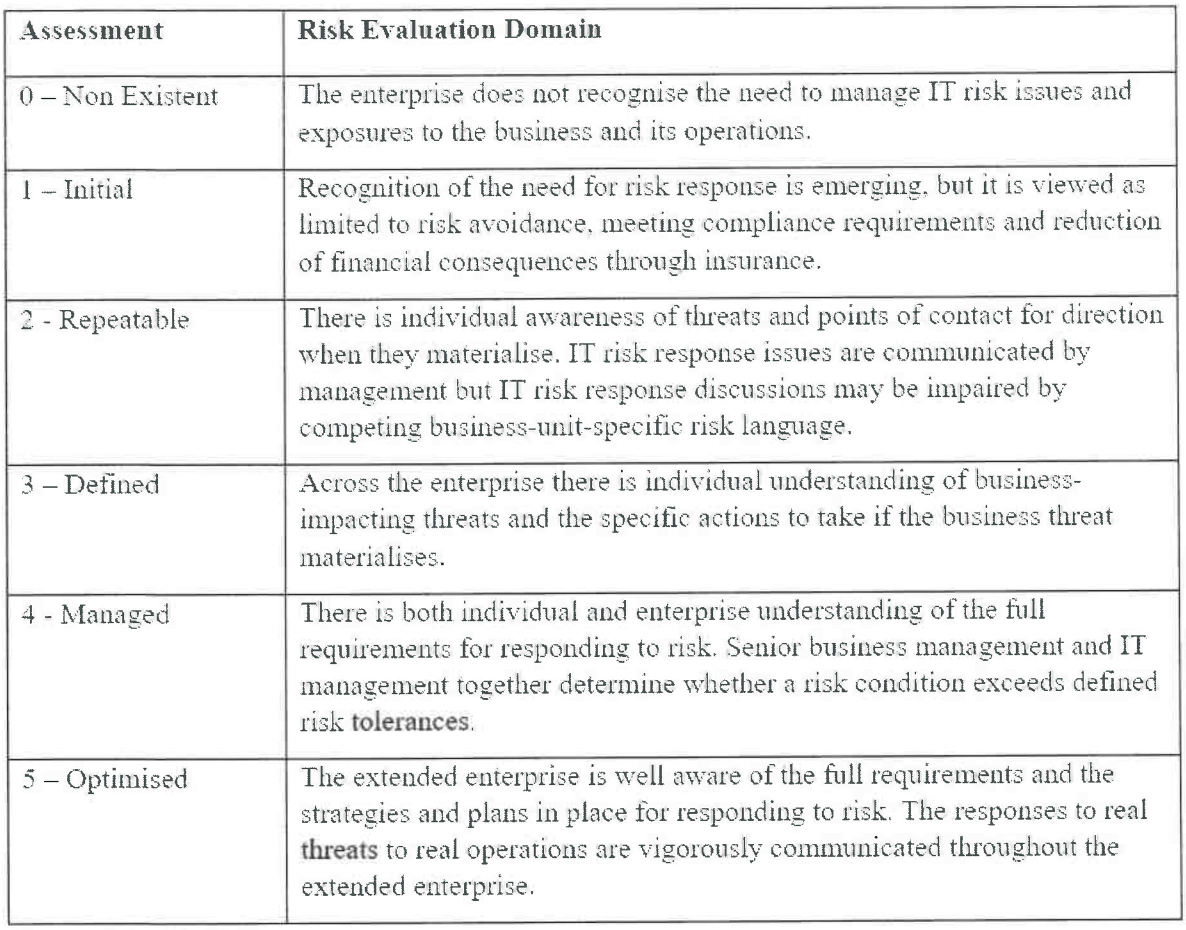
Based on this score, it can be derived that regulated entities that provide mobile lending have a thorough understanding of risk essentials. In technology risk evaluation for regulated entities, gaps between ICT risk and opportunity are recognised and addressed on a continuous basis.

For unregulated entities, the recognition of the need for risk evaluation is limited and it highlights gaps in processes that may be consequential to the performance of the mobile lending business.

4.5.4 Analysis of Adequacy in Risk Response

The RiskIT framework by ISACA provides for the following assessment model:

Table 11: Risk Response Maturity Model



Assessment	Risk Evaluation Domain
0 – Non Existent	The enterprise does not recognise the need to manage IT risk issues and exposures to the business and its operations.
1 – Initial	Recognition of the need for risk response is emerging, but it is viewed as limited to risk avoidance, meeting compliance requirements and reduction of financial consequences through insurance.
2 - Repeatable	There is individual awareness of threats and points of contact for direction when they materialise. IT risk response issues are communicated by management but IT risk response discussions may be impaired by competing business-unit-specific risk language.
3 – Defined	Across the enterprise there is individual understanding of business-impacting threats and the specific actions to take if the business threat materialises.
4 - Managed	There is both individual and enterprise understanding of the full requirements for responding to risk. Senior business management and IT management together determine whether a risk condition exceeds defined risk tolerances.
5 – Optimised	The extended enterprise is well aware of the full requirements and the strategies and plans in place for responding to risk. The responses to real threats to real operations are vigorously communicated throughout the extended enterprise.

Source: ISACA, 2009

Based on a score of 1 to 5, entities were scored for each of the domain activities based on their answers to different aspects of technology risk governance.

Table 12: Risk Response Activity Scoring

Domain Activity	Regulated	Unregulated
RR1.1 Communicate IT risk analysis results	3.27	1.25
RR1.2 Report IT risk management activities	3.00	1.10
RR1.3 Interpret independent IT assessment findings	3.07	1.20
RR1.4 Identify IT-related opportunities	3.13	2.85
RR2.1 Inventory controls	3.13	2.85
RR2.2 Monitor operational alignment with risk tolerance	3.10	2.75
RR2.3 Respond to discovered risk exposure and opportunity	3.17	1.25
RR2.4 Implement controls	3.00	2.65
RR2.5 Report IT risk action plan progress	3.30	1.40
RR3.1 Maintain incident response plans	2.93	2.70
RR3.2 Monitor IT risk	4.17	1.00
RR3.3 Initiate incident response	5.00	5.00
RR3.4 Communicate lessons learned from risk events	2.53	3.00
Average Score	**3.29**	**2.23**
Risk Rating	**Medium**	**Medium**

Source: Research Data, 2019

Based on this score, it can be argued that for regulated entities, across the enterprise, there is a top-down organizational awareness of technology threats and an understanding of what response mechanisms to undertake. This is commendable as it shows that through technology governance and strengthened ICT risk evaluation mechanisms, risk responses are well defined and executable.

For unregulated entities, while there is room for more awareness of technology threats and exploitable weaknesses. The lack of continuous monitoring hampers any effective risk response and mitigation strategies. This is because the business-unit-specific risk language creates an environment that would affect the collective efficiency of technology risk response efforts.

4.5.5 Relationship Analysis using Correlation and Regression

Below are the hypotheses that informed this study:

i. **Hypothesis 1** – IT risk governance has a significant influence on the adequacy of technology risk management.

ii. **Hypothesis 2** – IT risk evaluation has an influence on the adequacy in technology risk management.

iii. **Hypothesis 3** – IT risk response mechanisms have an effect on the adequacy in technology risk management.

iv. **Hypothesis 4** – Whether a firm is regulated or not has an effect on adequacy of technology risk management

Data was aggregated per domain and transformed to present a statistical analysis framework. Each of the responses was scored and calibrated to percentages as shown below:

Type	IT Risk Governance	IT Risk Evaluation	IT Risk Response	Aggregated Score	Perception
Regulated	82.67%	67.94%	65.85%	72.15%	100.00%
Unregulated	27.62%	10.64%	44.62%	27.62%	50.00%

Source: Research Data, 2019.

Table 13: Assessment of Perception

Type	Evaluation	Governance	Response	Average	Perception
Tier 1 Bank	0.69	0.88	0.68	0.75	1.00
Mobile App	0.11	0.49	0.45	0.35	0.50
Tier 1 Bank	0.70	0.89	0.68	0.76	1.00
Tier 1 Bank	0.69	0.86	0.68	0.74	1.00
Tier 1 Bank	0.69	0.88	0.68	0.75	1.00
MFI	0.59	0.57	0.54	0.57	1.00
Tier 1 Bank	0.71	0.87	0.68	0.75	1.00
Mobile App	0.09	0.14	0.47	0.24	0.50
Mobile App	0.11	0.12	0.41	0.22	0.50
Mobile App	0.11	0.34	0.45	0.30	0.50

Source: Research Data, 2019.

The variables were mapped for regression analysis as illustrated below:

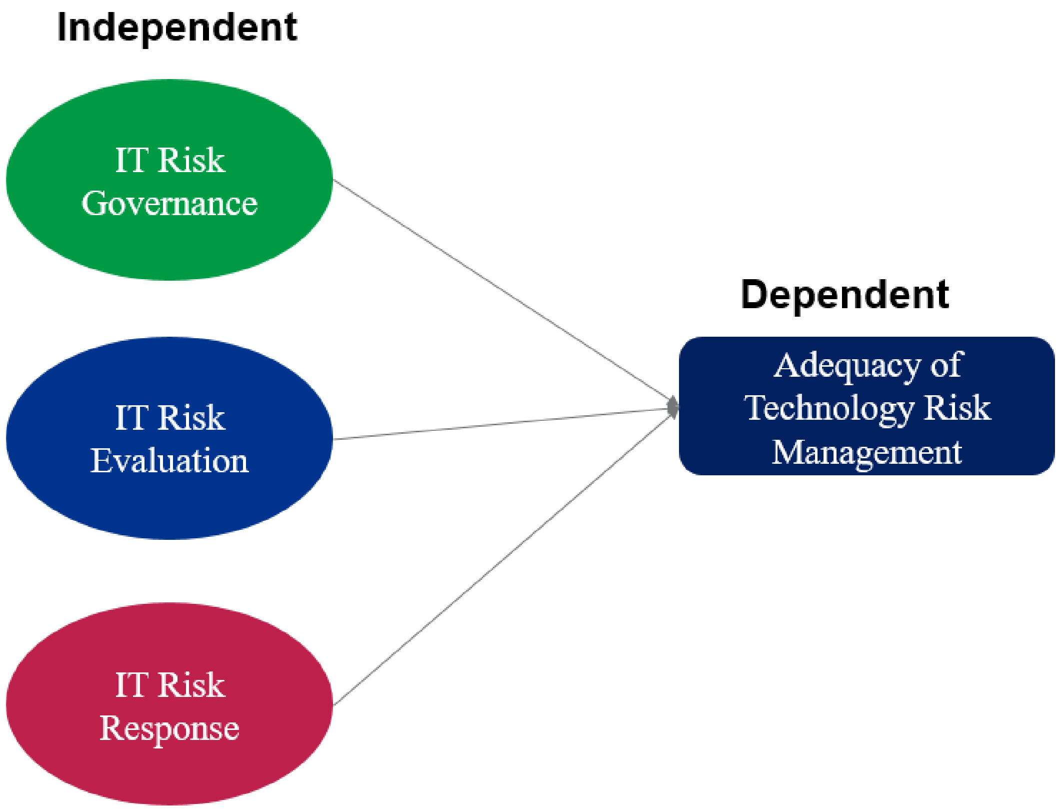
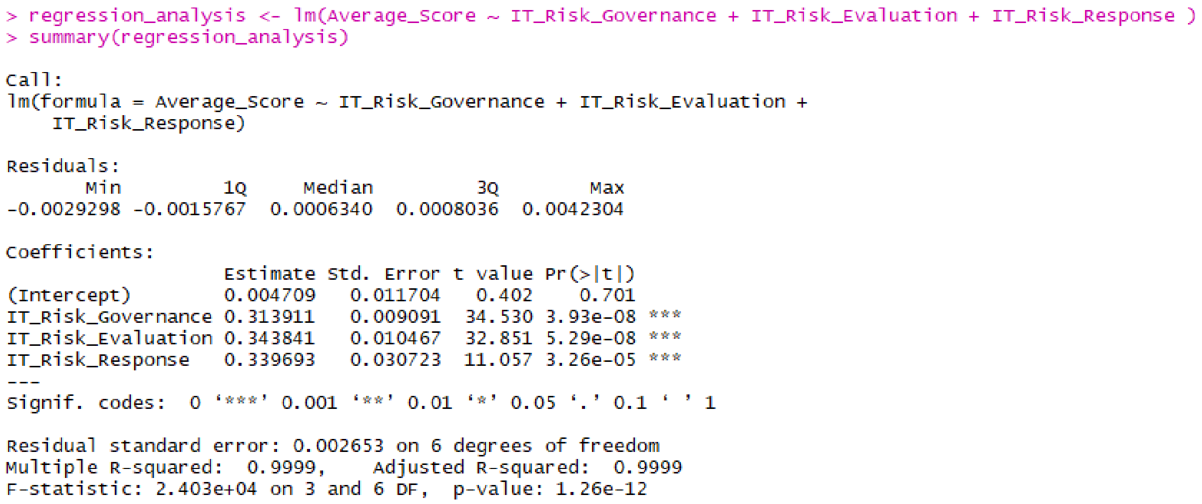


Figure 4: Mapping of Variables for Regression Analysis

The results based on the data and analysis done in R is as below:



```
> regression_analysis <- lm(Average_Score ~ IT_Risk_Governance + IT_Risk_Evaluation + IT_Risk_Response )
> summary(regression_analysis)

Call:
lm(formula = Average_Score ~ IT_Risk_Governance + IT_Risk_Evaluation +
    IT_Risk_Response)

Residuals:
       Min         1Q     Median         3Q        Max 
-0.0029298 -0.0015767  0.0006340  0.0008036  0.0042304 

Coefficients:
                   Estimate Std. Error t value Pr(>|t|)    
(Intercept)        0.004709   0.011704   0.402    0.701    
IT_Risk_Governance 0.313911   0.009091  34.530 3.93e-08 ***
IT_Risk_Evaluation 0.343841   0.010467  32.851 5.29e-08 ***
IT_Risk_Response   0.339693   0.030723  11.057 3.26e-05 ***
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1

Residual standard error: 0.002653 on 6 degrees of freedom
Multiple R-squared:  0.9999,	Adjusted R-squared:  0.9999 
F-statistic: 2.403e+04 on 3 and 6 DF,  p-value: 1.26e-12
```

Figure 5: Regression Analysis - Test of Hypothesis

Based on the regression output from R, the null hypothesis is rejected. It can be proven that IT risk governance, evaluation and response have a significant influence on the adequacy of technology risk management.

Table 14: Coefficients from Regression Analysis

	Estimate	**Std. Error**	**t value**	**Pr (>|t|)**
(Intercept)	0.004708531	0.011704367	0.402288415	0.701411503
IT Risk Governance	0.313911352	0.009091094	34.52954467	0.000000039
IT Risk Evaluation	0.343840972	0.010466818	32.85057386	0.000000053
IT Risk Response	0.339693034	0.030722567	11.05679196	0.000032574

Source: Research Data, 2019.

An increase in any of the independent variables would lead to an increase in adequacy of technology risk management.

A multiple R of 0.99 indicates a strong positive relationship between adequacy of technology risk management and variables of interest namely: governance, evaluation and response.

An R Square of 0.99 indicates that 99% of the changes in the technology risk management adequacy can be explained by how an organization manages its IT risk governance, evaluation and response.

The model p-values and the individual variable p-values are less than 5%. This shows that both the model and the variables are statistically significant (p>0.05).

Hypothesis 4 – Whether a firm is regulated or not has an effect on adequacy of technology risk management was also proven through the evaluation of survey responses and the average scoring per domain.

Qualitatively, it was also evident that regulation is a key factor in the assessment of how each entity fulfilled the requirements of the domains of the RiskIT framework.

Type	IT Risk Governance	IT Risk Evaluation	IT Risk Response	Average Score	Perception
Regulated	82.67%	67.94%	65.85%	72.15%	100.00%
Unregulated	27.62%	10.64%	44.62%	27.62%	50.00%

Source: Research Data, 2019

4.5.6 Respondent Perception of Adequacy in Technology Risk Management

Based on research data collected, respondents were requested to provide feedback if they considered technology risk management at their organizations to be adequate.

In light of the responses you have provided above, do you consider technology risk management at your mobile lending organization to be adequate?

	Regulation		Total
	Regulated	Unregulated	
Yes	100.0%	50.0%	80.0%
No		50.0%	20.0%
Total	100.0%	100.0%	100.0%

Source: Research Data, 2019.

4.5.7 Relationship of Independent Variables to Perception of Adequacy

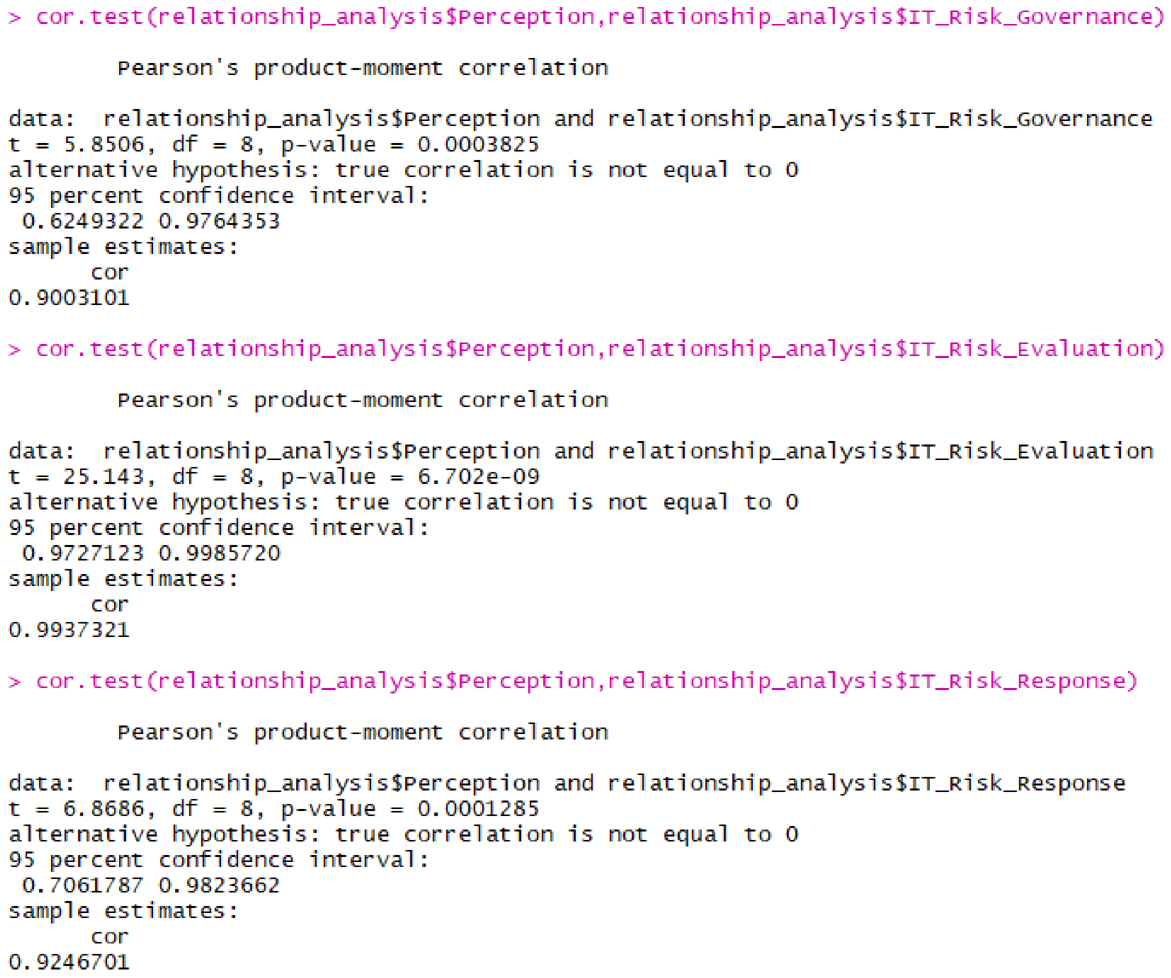
A correlation analysis was done to determine the relationship between risk governance, evaluation and response to the perception of adequacy by the respondents.

Table 15: Summary of Correlation Analysis

Domain	**Perception of Adequacy**
IT Risk Evaluation	0.9937
IT Risk Governance	0.9003
IT Risk Response	0.9247

Source: Research Data, 2019

The detailed R output is shown below:



```
> cor.test(relationship_analysis$Perception,relationship_analysis$IT_Risk_Governance)

        Pearson's product-moment correlation

data:  relationship_analysis$Perception and relationship_analysis$IT_Risk_Governance
t = 5.8506, df = 8, p-value = 0.0003825
alternative hypothesis: true correlation is not equal to 0
95 percent confidence interval:
 0.6249322 0.9764353
sample estimates:
      cor 
0.9003101 

> cor.test(relationship_analysis$Perception,relationship_analysis$IT_Risk_Evaluation)

        Pearson's product-moment correlation

data:  relationship_analysis$Perception and relationship_analysis$IT_Risk_Evaluation
t = 25.143, df = 8, p-value = 6.702e-09
alternative hypothesis: true correlation is not equal to 0
95 percent confidence interval:
 0.9727123 0.9985720
sample estimates:
      cor 
0.9937321 

> cor.test(relationship_analysis$Perception,relationship_analysis$IT_Risk_Response)

        Pearson's product-moment correlation

data:  relationship_analysis$Perception and relationship_analysis$IT_Risk_Response
t = 6.8686, df = 8, p-value = 0.0001285
alternative hypothesis: true correlation is not equal to 0
95 percent confidence interval:
 0.7061787 0.9823662
sample estimates:
      cor 
0.9246701 
```

Figure 6: Correlation Analysis

The results show that the independent variables are strongly and positively correlated to the dependent variable with statistically significant p-values.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

This chapter provides a summary of the findings, conclusions, suggestions for further research and recommendations to all stakeholders regarding strengthening technology risks management in mobile money lending. It also includes a research assessment framework that provides a view into why this study is beneficial to various players.

5.1 Summary of Findings

In summary, a majority of respondents recognize the value of technology risk management in digital lending. However, they believe that their ICT and risk functions are not entirely effective in readiness for complex technology challenges in their enterprises.

The study shows that regulated environments are more robust in practice of technology risk management, their processes are defined and linked to specific organizational objectives. Unregulated environments do not have the same level of awareness and application of technology risk management practices. This presents a risk in the mobile lending ecosystems as it could lead to materialization of threats such as cyber-attacks, loss of revenue, terrorism financing, and reputation loss. Events like these would damage consumer confidence.

Introduction of new concepts and ways of optimising business processes presents new challenges. In the interview of respondents, a part of the digital lending force believes that rapid advances in technology are increasingly threatening stability of the lending landscape and to manage risks, you need the right people and investment. Respondents recognize that it is a challenge to identify the right people with the skills that match the technology risk management requirements of a fast changing technology world.

Further, having the investment required to drive technology risk initiatives across the enterprise is a key success factor. 94% of the respondents noted that there is none or minimal investment in robust technology risk frameworks since they had experience resource constraints in their efforts to enable technology risk management.

On a scale of 1 to 5 that was informed by the RiskIT practitioner's guide, each activity under the process areas was scored with the results as below:

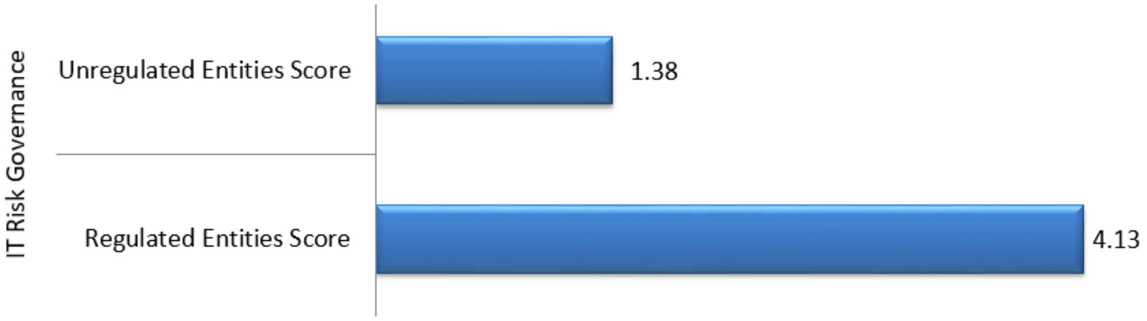
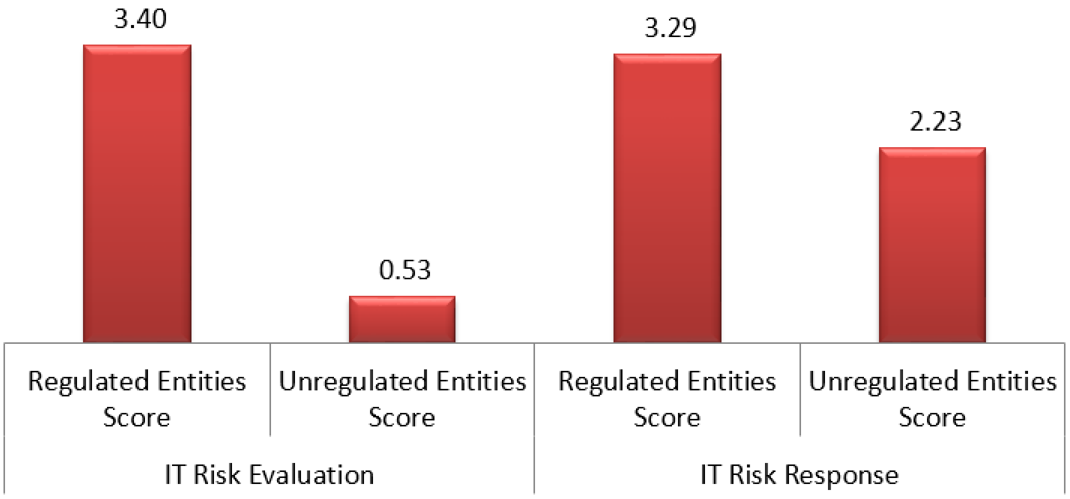


Figure 7: Comparison of Risk Governance Performance

Regulated entities outperform their unregulated competitors. In assessing the adequacy of technology risk management in regulated and unregulated digital lending environments, a review was done on evaluation and response mechanisms.

The results shown below show that for regulated entities, there is a thorough understanding of technological threats and the actions in response of the harm they are likely to cause.

For unregulated entities there is opportunity for growth and development in this area. Gaps were identified that expose weaknesses in evaluation of technology risks and responses in a timely manner. These gaps could be exploited and expose the firms to loss of revenue and reputation.



***Sample Size of 50 respondents across banks and mobile lenders**

Figure 8: IT Risk Evaluation and Response Comparison

5.2 Linking Findings to the Objectives

Research Objective 1*: Identify technology risk management practices in entities that offer mobile money lending.*

Guided by literature review in Chapter 2 and use of the RiskIT framework, the review revealed some of the factors that must be adhered to in order to mitigate risks associated with information technology enabled lending. These include risk governance, risk evaluation and risk response. The study shows that the digital lending industry does not have standardized risk management practices and instead, each entity is focused on its internal processes.

Research Objective 2: *Assess adequacy of technology risk management in regulated and unregulated digital lending environments*

Through questionnaires, data was collected on the adequacy of technology risk management for both regulated and unregulated lenders. The study shows that there are gaps in technology risk management for unregulated mobile lenders. These gaps expose weaknesses in governance of technology risk management, evaluation and response.

Research Objective 3: *Propose appropriate strategies that would help mitigate the risks associated with technology enabled lending. This objective was answered in Section 5.3 below.*

Based on the research findings, it has been proposed that to ensure technology risk management capabilities are robust, the key considerations for all mobile money lending institutions would include: Alignment of Technology Risk Management with Enterprise Risk, Adoption of a business driven approach in IT Risk Management, Culture: Enabling IT to drive business success, Anticipation of IT Risk, Embedding IT Risk Management into existing processes.

5.3 Strategies to Mitigate Technology Risks in Mobile Lending

In a report on technology risks by the Data Centre Frontier, (Data Centre Frontier, 2016), the average cost of recovery from technology risks has steadily increased over the last decade. Given the rapid evolution of technology and continued progression, organizations are encouraged to evolve their risk management, security and compliance capabilities and to avoid technology incidents that are counter-productive to business goals.

The following strategies have been proposed based on the framework recommendations, findings and the noted weaknesses in technology risk management:

5.3.1 Alignment of IT Risk Management with Enterprise Risk

Similar to the requirements of the RiskIT framework on alignment of IT Risk Management to Enterprise Risk Management, it is critical that technology risk management efforts are aligned with the overall objectives of enterprise risk management.

There are multiple parties in any organization that are focused on risk management. These include risk management, internal audit, information security and cyber security. It is important that all of these parties are aligned on risk categorization, processes, response activities and definition of impact to the organization. The alignment can be achieved through relationship management, collaboration, and having a deliberate interactive approach across all the relevant teams.

5.3.2 Adoption of a business driven approach in IT Risk Management

It is key for all entities to recognize that IT risk management just focused on technology in a silo will fail to deliver required benefits. Conscious efforts must be made to ensure that IT risk management enables and protects current and future needs of the business. For example, working with the business to identify the areas and new ventures where there is a low appetite for risk will help IT prioritize its efforts to high risk areas.

To achieve this, IT risk processes should be made more consistent with a deeper dive on ensuring that there is technology supporting higher risk business areas. Formal metrics and results monitoring should be maintained so that an environment is created where technology risk management is working hand-in-hand with the business to drive growth.

5.3.3 Culture: Enabling IT to drive business success

Technology risk management programs are most successful when they are positioned as an enabler to IT to help drive quality services to the business so that the business can achieve their strategic objectives.

One of the ways to improve on culture and awareness is to make effort on the messaging across the enterprise on the role of IT risk management. This will increase the level of ownership and accountability in a shorter amount of time and drive the risk-minded culture that an organization should have.

To prepare a workforce that is IT risk management aware, it is imperative for all functions to provide opportunities for staff to learn and develop their skills in line with initiatives for technology risk management.

5.3.4 Anticipation of IT Risk

Forward looking IT risk reporting can improve both risk mitigation and operational efficiency by bringing a focus to key IT risks and trends. This is critical for effective IT risk management. Intelligent reporting and anticipation provides a basis for enhanced decision-making around key IT risks and ultimately commitment on treatments and actions.

There are some suggested ways this can be achieved. Reliable data collection and quick assembly through predictable and repeatable methodology and sources of data enables IT risk reporting capabilities at multiple levels of the enterprise such as process level, line of business, country, region, strategic business entity among others.

5.3.5 Embedding IT Risk Management into existing processes

Technology risk processes must align with how IT is structured and managed. It is key for technology risk management to make efforts of increasing effectiveness by collaborating with existing IT processes and data sources.

One of the ways to achieve this is to start small in areas of highest risk but going deep so as to drive insights and ultimately credibility. Further, investment by all stakeholders is required to ensure the envisioned success.

5.4 Research Assessment Framework

There is a solid case to be made as to why digital lending, technology risk management and regulation are areas to concern various stakeholders and researchers.

In Kenya, the Central Bank of Kenya (CBK) continues to voice its concerns (Reuters, 2018) and play its role of enabling a strong regulatory framework (Muthiora, 2015). Further, the National Payment Systems (NPS) Act and NPS Regulations in August 2014 provided an enabling ecosystem for mobile and payments innovations (Central Bank of Kenya, 2011).

There is general consensus among many players in digital financial services that through mobile money lending, those excluded from current financial systems have access and opportunity to make their lives better (Björkegren & Darrell, 2018). However, other researchers have questioned policy-makers' expectations that mobile money is able to swiftly integrate to the social and economic value-chain (Johnson, 2016).

In light of the above, this thesis makes a significant contribution by not only recognizing the value of mobile money lending as contributed by a broad intersection of researchers, but also highlighting the pitfalls that mobile lending practitioners should be aware of, particularly in technology risk management.

With regards to financial technology, there have been some suggested countermeasures for network credit risk (Zhang, 2018), this research enriches that body of knowledge by adding perspectives of governance within a globally practiced framework of technology risk management. This research also challenges mobile money lenders and regulators to take a focus and interest in every aspect of the practice to ensure a robust lending ecosystem.

There is underlying evidence as to why this is important. For example, a particular question arises, would a terrorist keen on inflicting pain have access to a mobile loan? Various scholars have highlighted that weaknesses in controls enable the materialization of potential dangers of terrorism financing (Levi, 2010), one way of ensuring this does not get propagated through mobile lending is to review and regulate the practice within a framework so that it cannot be an enabler of any vice (Buku & Meredith, 2012). In addition, regulation is key, researchers have shown that markets with continuous regulatory scrutiny and policy making enjoy greater benefits in their financial access enablement initiatives (GSMA, 2016).

This study has been made through a thorough review of the mobile lending ecosystem in the Kenya, linked literature by scholars and supporting practices as advised by various professionals in the trade. The thesis is structure and written to ensure the reader can align the growth in financial technology to the pertinent issues that must be addressed by all stakeholders.

5.5 Limitations of Study

The research was limited to the top lenders in regulated entities and additional unregulated lenders. Therefore, respondents from other tiers of lending who provide credit to the informal sector were left out. Further, the location of all the respondents was Nairobi, Kenya's Capital City.

Acquiring all the comprehensive datasets considered important to the study such as credit scoring practices from the lenders was not possible. This is because the lenders consider their customer assessment techniques to be proprietary.

5.6 Suggestions for Further Study

Based on the findings of this study, it is recommended that for more efforts are made towards reviewing and assessing finance operating models including organization structures and governance for unregulated mobile money lenders.

An understanding of the strategies of the two environments (regulated and unregulated) would also be useful in deciphering what drives the technology risk management and related initiatives within the specific enterprises.

It is also advised for further study, that contribution towards policies be made that necessitates the mobile money lending industry to evaluate their customer due diligence measures. This will further contribute to research efforts for technology risk assessment especially in use cases of money-laundering and terrorism financing.

In addition, in the East Africa market, it is important to understand a firm's internal controls and technology systems that are in place to guard against such activities like financial crimes and money laundering prior to licencing its operations in the market, this is an additional recommended area of further study.

REFERENCES

Adem, O., Gichuhi, A. W., & Otieno, R. O. (2012). Parametric Modeling of Probability of Bank Loan Default in Kenya. *Journal of Agriculture,Science and Technology, 14*(1), 61 – 74.

Aduda, J., & Gitonga, J. (2011). The Relationship between Credit Risk Management and Profitability among the Commercial Banks in Kenya. *Journal of Modern Accounting and Auditing, 7*(9).

Ahlan, A. (2012). Information Technology Risk Management: The case of the International Islamic University Malaysia. *Journal of Research and Information in Information Systems*, 58-67.

Ali, R., Barrdear, J., Clews, R., & Southgate, J. (2014). Innovations in Payment Technologies and the Emergence of Digital Currencies. *Bank of England Quarterly Bulletin, 54*(3), 262-275.

Al-Jabri, I., & Sohail, S. (2012). Mobile Banking Adoption: Application of Diffusion of Innovation Theory. *Journal of Electronic Commerce Research, Vol. 13, No. 4*, 371 - 396.

Allen, F., Carletti , E., Cull, R., Qian, J., Senbet, L., & Valenzuela, P. (2013). *Improving access to banking. Evidence from Kenya.* Washington, DC.: World Bank. Retrieved from http://hdl.handle.net/10986/16044

Alliance for Financial Inclusion. (2012). *AFI Global*. Retrieved from AFI Global Website: https://www.afi-global.org/news/2012/11/safaricom-cba-launch-groundbreaking-mobile-banking-service-m-shwari

Almari, A. (2002). *The Credit Evaluation Process and the Role of Credit Scoring: A Case Study of Qatar.* Dublin: University College Dublin.

Azjen. (1985). *From intentions to actions:A theory of planned behaviour.* New York: Springer-Verlag.

Bamwesigye, J. (2008). *Microfinance and Poverty Reduction in Rwanda: A case of Urwego Opportunity Microfinance Bank.* Thesis (Maters Degree). Retrieved February 25, 2019, from https://thesis.eur.nl/pub/7054/Bamwesigye%20PPSD%202007-08.pdf

Beck, T., Demurgic-Kunt, A., & Martinez, P. M. (2007). *Banking services for Everyone? Barriers to Bank Access and Use around the world.* Washington, D.C: World Bank.

Bernard, H. R. (2000). *Social research methods : qualitative and quantitative approaches.* Thousand Oaks, California: Sage Publiactions.

Björkegren, D., & Darrell, G. (2018). The Potential of Digital Credit to Bank the Poor. *AEA Papers and Proceedings, 108,* 68 -71.

Blechman, J. G. (2016). Mobile credit in Kenya and Tanzania: Emerging regulatory. *The African Journal of Information and Communication (AJIC).*

Bolton, C. (2013). *Logistic Regression and its application in credit scoring.* Pretoria: University of Pretoria.

Bryman, A., & Bell, E. (2011). *Business Research methods* (4th Edition ed.). London: Oxford University Press.

Brynjolfsson, E., Hitt, L. M., & Bresnahan, T. F. (2002). Information technology, workplace organization, and the demand for skilled labor: Firm-level evidence. *The Quarterly Journal of Economics, 117*(1), 339-376.

Brynjolfsson, E., Malone, T. W., Gurbaxani , V., & Kambil, A. (1994). Does Information Technology Lead to Smaller Firms? *Management Science, 40*(12), 1628-1644.

Buku, M., & Meredith, M. (2012). Safaricom and M-Pesa in Kenya: financial inclusion and financial integrity. *8 Wash. J. L. Tech. & Arts 375*.

Burtch, G., Ghose, A., & Wattal, S. (2013). *Cultural Differences and Geography as Determinants of Online Pro-Social Lending.* Retrieved from MIS Quarterly, Forthcoming; Fox School of Business Research Paper No. 14-021. : http://dx.doi.org/10.2139/ssrn.2271298

Can, E., & Gansmann, A. (2015). *A semi-parametric Probability of Default Model*. Retrieved from http://arc.hhs.se/download.aspx?MediumId=2818

Cassar, D. (2018, January 25). Retrieved February 19, 2019, from IAPSS: https://iapss.org/2016/01/25/demystifying-the-economic-growth-elixir-growth-without-development/

Central Bank of Kenya. (2011). *National Payments System Act.* Retrieved from Central Bank of Kenya Website: https://www.centralbank.go.ke/images/docs/legislation/NATIONAL%20PAYMENT%20SYSTEM%20ACT%20(No%2039%20of%202011)%20(2).pdf

Central Bank of Kenya. (2017). *Banking Supervision Report.* Nairobi, Kenya: Central Bank of Kenya.

Chatian, P. L., Zerzan, A., Noor, W., Dannaoui, N., & De Koker, L. (2016). *Internet, Finance and Development.* Washington, D.C: World Bank.

Chau, P. K., & Kuan, K. Y. (2001). A perception-based model for EDI adoption in small businesses using a technology–organization–environment framework. *Information & Management, 38*(8), 507-521.

Chau, P., & Kar, T. Y. (1997). Factors Affecting the Adoption of Open Systems: An Exploratory Study. MIS Quarterly. *MIS Quarterly*, 1 - 21.

Chiang, W. K., Zhang , D., & Zhou, L. (2006). Predicting and explaining patronage behaviour toward web and traditional stores using neural networks: A comparative analysis with logistic regression. *Decison Support Systems, 41*(2), 514-531.

Consultative Group to Assist the Poor (CGAP). (2017). *Serving Smallholder Farmers: Recent Developments in Digital Finance.* Washington, DC: Consultative Group to Assist the Poor (CGAP).

Creswell, J. (2014). *Research design: Qualitative,Quantitative and Mixed Methods Approcahes* (4th ed.). Washington, D.C: Sage Publications.

Crook, J. (1996). Credit scoring: An overview. *European Journal of Operational Research, 95*, 24-37.

Crook, J., Overstreet, G., & Desai, V. (1996). A Comparison of Neural Networks and Linear Scoring Models in the Credit Union Environment. *European Journal of Operational Research., 95*(1), 24-37.

Crowther, D., & Lancaster, G. (2008). *Research Methods: A Concise Introduction to Research in Management and Business Consultancy.* (2nd ed.). London: Elsevier Butterworth-Heinneman .

Dasgupta, C., Dispensa, G., & Ghose, S. (1994). Comparing the predictive performance of a neural network model with some traditional market response models. *International Journal of Forecasting., 10*(2), 235-244.

Data Centre Frontier. (2016). *Data Center Costs*. Retrieved from https://datacenterfrontier.com/cost-of-data-center-outages/

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-340.

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly, 13*(3), 319-340.

Delmas, M. A. (2002). The diffusion of environmental management standards in Europe and in the United States: An institutional perspective. *Policy Sciences, 35*(1), 91-119.

Demirkan, H., & Harmon, R. (2009). Service Oriented Technology in Healthcare Services: A Research Framework for Studying the Computerized Physician Order Entry System. *PICMET 2009 Proceedings.* Portland, Oregon, USA.

DePietro, R., Wiarda, E., & Fleischer, M. (1990). The Context for Change: Organization, Technology, and Environmental. In L. G. Tornatzky, & M. Fleischer, *The Process of Technological Innovation* (pp. 151-175). Boston: Lexington Books.

DeYoung, F., Glennon, D., & McMillen, D. (2008). Commercial lending distance and historically underserved area. *Journal of Economics and Business, 60*(1-2), 149-164.

Dombora, S. (2016). *Characteristics of information security implementation methods.Volume of Management, Enterprise and Benchmarking in the 21st Century III.* Óbuda University, Keleti Faculty of Business and Management.

Donou-Adonsou, F., & Slywester, K. (2016). Financial Development and poverty reduction in developing countries: New evidence from banks and microfinance institutions. *Review of Development Finance, 6*(1), 82-90.

Dwived. (n.d.).

Dwivedi, Y. K., Nripendra, R. P., Anand, J., Clement, M., & Williams, M. D. (2017). Re-examining the Unified Theory of Acceptance and Use of Technology (UTAUT): Towards a Revised Theoretical Model. *Information Systems Frontiers,* 1-16.

Eposito, J. L. (n.d.). Interactive, multiple-method questionnaire evaluation research: A case study. . *Paper presented at the International Conference in Questionnaire Development, Evaluation, and Testing (QDET) Methods.* Charleston, SC.

Ertan , C., & Gansmann, A. (2015). *A semi-parametric Probability of Default model.* Stockholm: Stockholm School of Economics.

Esposito, J. L. (2004). Interactive, multiple-method questionnaire evaluation research: A case study. *Paper presented at the International Conference in Questionnaire Development, Evaluation, and Testing (QDET) Methods.* Charleston, SC.

Fosu, S. (2014). Credit information, consolidation and credit market performance: Bank-level evidence from developing countries. *International Review of Financial Analysis, 32,* 23-56.

Foundation for Development Cooperation. (2017). *Foundation for Development Cooperation*. Retrieved from Policy and Regulation: https://www.fdc.org.au/policy-and-regulation

Francis, E., Blumenstock, J., & Robinson, J. (2017). *Digital Credit: A Snapshot of the Current Landscape and Open Research Questions.* UC Berkeley.

FSD Africa. (2016). *The Growth of M-Shwari in Kenya – A Market Development Story.* Nairobi, Kenya: Financial Sector Deepening.

Galliers, R. (1991). Research issues in Information Systems. *Journal of Information and Technology*, 92 - 98.

Gallivan, M. (2001). Organizational adoption and assimilation of complex technological innovations: development and application of a new framework. *Information Systems - Special issue on adoption, diffusion, and infusion of IT,* 51-85.

Gibbs, J., & Kraemer, K. (2004). A cross-Country Investigation of the Determinants of Scope of ECommerce Use: An Institutional Approach. *Electronic Markets*, 124 - 137.

Gichuhi, A. O. (n.d.). *Parametric Modeling of Probability of Bank Loan Default in Kenya.*

Government of Kenya. (2009). *The Kenya Proceeds of Crime and Anti-Money Laundering Act*. Retrieved from The Kenya Proceeds of Crime and Anti-Money Laundering Act: http://www.frc.go.ke/downloads/download/10

Griffith-Jones, S., Karwowski, E., & Dafe, F. (2014). *A Financial sector to support development in low-income countries.* London: Overseas Development Institute.

Grossman, J., & Tarazi, M. (2014). *COE*. Retrieved from Criminal Money Flows on the Internet: Methods, Trends and MultiStakeholder Counteraction.: http://www.coe.int/t /dghl/monitoring/moneyval/

GSMA. (2016). *State of the Industry Report on Mobile Money Decade Edition: 2006 - 2016.* GSMA.

Gurak, H. (2015). Economic Growth and Development: Theories, criticisms and an alternative growth model. *PL Academic Research*.

Halty, M. (2002). Microfinance, Grants, and non-financial responses to poverty reduction: where does microcredit fit? *(Consultative Group to Assist the Poor*.

Hitt, L. (1999). An Empirically Derived Model for the Adoption of Customer-Based Interorganizational Systems. *Decision Sciences*, 603 - 639.

Hoti, E. (2015). The technological, organizational and environmental framework of IS innovation adaption in small and medium enterprises. Evidence from research over the last 10 years. *International Journal of Business and Management*, 1 - 14.

Hox, J., & Boeije H. (2005). Data Collection, Primary vs. Secondary. *Encyclopedia of Social Measurement*, 593.

Hussey, R., & Collis, J. (2013). *A practical guide for undergraduate and postgraduate students* (4th ed.). London: Palgrave Macmillan.

Iacovou, C., Benbasat, I., & Dexter, A. (1995). Information Technology and Firm Boundaries: Evidence From Panel Data. *Information Systems Research*, 134 - 149.

Infomineo. (2017). *Infomineo*. Retrieved from Mobile Banking and Why It's Growing in Africa: https://infomineo.com/mobile-banking-and-why-its-growing-in-africa

Information Systems Audit and Control Association. (2017). *CISA - ISACA Review Manual.* Information Systems Audit and Control Association.

Institute for Internal Auditors. (2007). *Guide to the Assessment of IT Risk.* New York: Institute for Internal Auditors.

International Finance Corporation. (2018). *DIGITAL ACCESS: The Future of Financial Inclusion in Africa.* Nairobi, Kenya: International Finance Corporation.

ISACA. (2009). *ISACA RIsk IT Framework*. Retrieved from http://www.isaca.org/KNOWLEDGE-CENTER/RESEARCH/RESEARCHDELIVERABLES/Pages/The-Risk-IT-Framework.aspx

ISO/IEC, ISO/FDIS 27005. (2008). *ISO/IEC, ISO/FDIS 27005.* International Organization for Standardization (ISO).

ISO/IEC, ISO/IEC27006. (2007). *Requirements for Bodies Providing Audit and Certification of Information Security Management Systems.* Switzerland: International Organization for Standardization (ISO).

Jack, W., & Suri, T. (2011). Mobile Money: The Economics of M-PESA. *NBER Working Paper No. 16721*, JEL No. O16,O33,O55.

Johnson, S. (2016). Competing visions of financial inclusion in Kenya: the rift revealed by mobile money transfer. *Canadian Journal of Development Studies/Revue canadienne d'études du développement*, 83 - 100.

Kalui, D., Muketha, G., Tarus, J., & Moturi, C. (2017). An Investigation into Customers' Requirements for Electronic Banking: A Case Study of Microfinance Institutions (MFIs) in Kenya. *International Journal of Innovation in the Digital Economy*, 39 - 54.

Keiser, N. F. (1975). *An introduction to growth theory; Macroeconomics.* New York: Random House.

Klapper, L. (2016). *Financial Inclusion has a big role to play in reaching the SDGs*. Retrieved from Consultative Group to Assist the Poor: http://www.cgap.org/blog/financial-inclusion-has-big-role-play-reaching-sdgs

Kombo, D., & Tromp, D. (2006). *Proposal and thesis writing: An Introduction.* Nairobi: Pauline's Publications Africa.

Korros, R. (2016). University Students Gambling: Examining the Effects of Betting on Kenyan University Students' Behavior. *International Journal of Liberal Arts and Social Science,* Vol 4 No 8.

Kuhl, J., Azjen, I., & Beckmann, J. (1985). *From intentions to actions: A theory of planned behavior in Action control: From cognition to behavior.* New York: Springer-Verlag.

Lacovou, C. (1995). Electronic Data Interchange and Small Organizations: Adoption and Impact of Technology. *MIS Quarterly 19, 19*(4), 465-485.

Levi, M. (2010). Combating the financing of terrorism: A history and assessment of the control of 'threat finance. *The British JOurnal of Criminology*, 650 - 669.

Li, Z., & Yang, S. (2016). Overview of risk management system of commercial bank data center. *International Journal of Security and Its Applications*.

M, A., Zain, J., Zolkipli, F., & Badshah, G. (2014). *Mobile Cloud Computing & Mobile Battery Augmentation Techniques: A survey*. Retrieved from Research Gate: http://www.researchgate.net/publication/270683821_Mobile_Cloud_Computing__Mobile_Battery_Augmentation_Techniques_A_Survey, 2014

Mbiti, I., & Weil, D. (2014). Mobile Banking: The impact of M-pesa in Kenya. *National Bureau of Economic Research. Working Paper No. 17129.*

McKee, K., Kaffenberger, M., & Zimmerman, J. (2015). Doing Digital Finance Right: The Case for Stronger Mitigation of Customer Risks. *CGAP, Focus Note 103*.

Miled, B., & Rejeb, B. (2015). Microfinance and Poverty Reduction; A review and synthesis of empirical evidence. *Social and Behavioural Sciences*, 705 - 712.

Mugenda, A. (2008). *Social Science Research: Theory and Principles.* Nairobi: Acts Press.

Muthiora, B. (2015). *Enabling mobile money policies in Kenya: Fostering a digital financial revolution.* . Retrieved from GSMA: https://www. gsma. com/mobilefordevelopment/programme/mobile-money/enabling-mobile-money-policies-in-kenya-fostering-a-digital-financial-revolution.

Njagi, L. (2009). *Effectiveness of Know Your Customer (KYC) Polices Adopted By Commercial Banks in Kenya in Reducing Money Laundering and Fraud Incidences.* Nairobi: University of Nairobi.

Ntibashirwa, C. (2013). *A Study on the Contribution of Microfinance Institutions in Reducing Financing Constraints for the promotion of small and medium sized enterprises.* Nairobi: University of Nairobi.

Nyasimi, E. (2016). *Effects of mobile money transfer services on economic growth in Kenya.* Nairobi: University of Nairobi.

Oates, B. (2006). *Researching information systems and computing.* London: Sage.

Ogechi, A., & Olaniyi, E. (2012). Financial Inclusion, Financial Development and Economic Diversification in Nigeria. *Journal of Developing Areas*, 2 - 15.

Orodho, J. (2009). *Techniques of writing research proposals and reports in education and social sciences.* Nairobi: Kanezja Publishers.

Papworth, T. (2014). The role of finance in inclusive growth. *Centre Forum Organization*, 1-3.

Porter, M., & Millar, V. (1985). How Information Gives You COmpetitive Advantage. *Harvard Business Review*, 145 - 160.

Reuters. (2018). *Kenya's central bank governor calls for regulation of fintech lenders*. Retrieved from Reuters - Fintech: https://www.reuters.com/article/us-kenya-fintech/kenyas-central-bank-governor-calls-for-regulation-of-fintech-lenders-idUSKCN1IU0N4

Rogers, E. (2003). *Diffusion of Innovations, 5th Edition.* Simon and Schuster.

Ruefle, R., Dorofee, A., Mundie, D., Householder, A., Murray, M., & Perl, S. (2014). Computer Security Incident Response Team Development and Evolution. *IEEE Security & Privacy, Vol. 12, No. 5*, 16 - 26.

Safaricom M-PESA. (2019, January). *Safaricom PLC*. Retrieved from Safaricom MPESA: https://www.safaricom.co.ke/personal/m-pesa

Saunders, M., Lewis, P., & Thornhill, A. (2012). *Research methods for business students. 6th edition.* Harlow, New York: Pearson.

Savings Groups Information Exchange. (2016). *Savings Groups Information Exchange*. Retrieved from Savings Groups Information Exchange Database: http://www.thesavix.org/.

Sen, A. (1999). *Development as freedom.* New York: A Knopf.

Sinha, A. (2012). Sinha, Anand, Financial Sector Regulation and Implications for Growth (January 1, 2012). BIS Paper No. 62G. . *https://ssrn.com/abstract=2021108*.

SVBIC. (2011). *SVBIC*. Retrieved from What is Economic Development?: http://www.svbic.com/node/24

Taber, K. (2018). Resources Science Education. *https://doi.org/10.1007/s11165-016-9602-2,* 48.

Tanzania Invest. (2018). *Tanzania Mobile Money*. Retrieved from Tanzania Invest: https://www.tanzaniainvest.com/mobile-money

The Economist. (2015). *Why does Kenya lead the world in mobile money?* . Retrieved from The Economist: https://www.economist.com/the-economist-explains/2015/03/02/why-does-kenya-lead-the-world-in-mobile-money

The Global Public Policy Committee. (2016). *The Auditor's Response to the Risks of Material Misstatement Posed by Estimates of Expected Credit Losses under IFRS 9.* GPPC.

The World Bank - Council of Europe. (2012). Protecting Mobile Money against Financial Crimes. *Global Policy Challenges and Solutions*.

The World Bank. (2017, December). *Financial Inclusion*. Retrieved from Financial Inclusion, An Overview: http://www.worldbank.org/en/topic/financialinclusion/overview

Tornatzky, L., & Fleischer, M. (1990). *The Processes of Technological Innovation.* Massachusetts: Lexington Books, Lexington,.

Totolo, E. (2018). *The Digital Credit Revolution in Kenya: An Assessment of Market Demand, 5 Years On.* Retrieved from Financial Sector Deepening Trust Kenya (FSDK): https://www.findevgateway.org/library/digital-credit-revolution-kenya-assessment-market-demand-5-years

Uday, K., & Aditya, P. (2009). Maintenance performance measurement (MPM): issues and challenges. *Journal of Quality in Maintenance Engineering, Vol. 12 Issue: 3,* 239 - 251.

United Nations. (2015). *United Nations*. Retrieved from Millenium Sustainable Development Goals: https://www.un.org/sustainabledevelopment/blog/2015/12/sustainable-development-goals-kick-off-with-start-of-new-year/

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, 425–478.

West, D. (2000). *Neural Network Credit Scoring Models. Computers & Operations Research.*

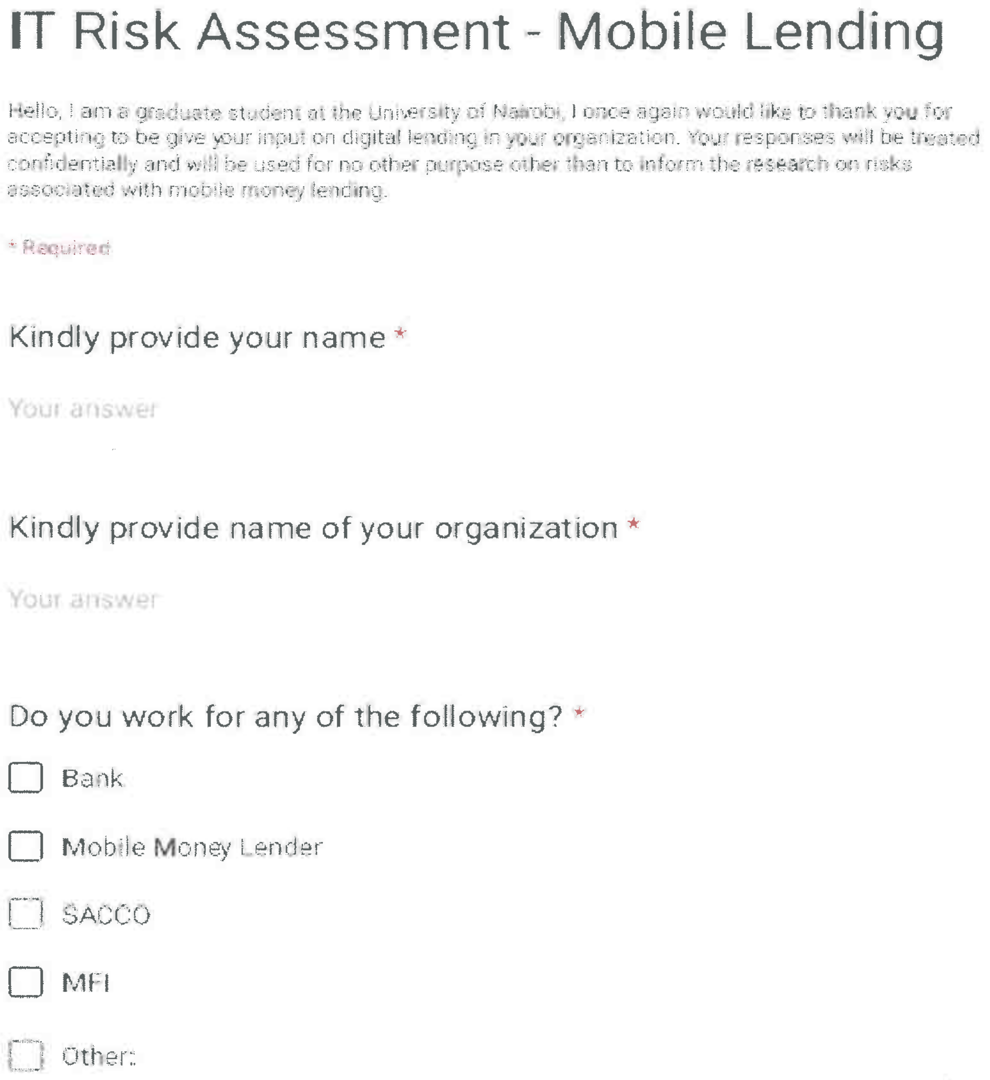
World Bank. (2017). *The Findex Global Database 2017.* Washington DC: The World Bank.

Zhang, D. (2018). Risk management analysis of network loan platform. *018 International Conference on Management, Economics, Education, Arts and Humanities (MEEAH 2018).*

Zhu, K., Kraemer, K., & Xu, S. (2006). The Process of Innovation Assimilation by Firms in Different Countries: A Technology Diffusion Perspective on E-Business. *Management Science*, 1557-1576.

Zikmund, W. (2012). *Business Research Methods - 9th Edition.* Ohio: South Western.

APPENDICES



IT Risk Assessment - Mobile Lending

Hello, I am a graduate student at the University of Nairobi, I once again would like to thank you for accepting to be give your input on digital lending in your organization. Your responses will be treated confidentially and will be used for no other purpose other than to inform the research on risks associated with mobile money lending.

* Required

Kindly provide your name *

Your answer

Kindly provide name of your organization *

Your answer

Do you work for any of the following? *

□ Bank

□ Mobile Money Lender

□ SACCO

□ MFI

□ Other:

Figure 9: Appendix 1 - Questionnaire Deployment

Table 16: Detailed Questionnaire Items

Process	**Activity**	**Questionnaire Item**
Risk Governance Domain		
Establish and Maintain a Common Risk View	RG1.1 Perform enterprise IT risk assessment	In the last financial year, have had an IT risk assessment or been made aware of one?
	RG1.2 Propose IT risk tolerance thresholds	Does your mobile lending business have documentation of the amount of IT related risk it can take?
	RG1.3 Approve IT risk tolerance	If available, are proposed IT risk tolerance thresholds approved?
	RG1.4 Align IT risk policy	Do you have an IT Risk Policy? If yes, do you agree that the policy aligns to business objectives?
	RG1.5 Promote IT risk-aware culture	How many IT risk related trainings have you undergone in the last 12 months?
	RG1.6 Encourage effective communication of IT risk	Does your organization maintain an IT risk communication plan?
Integrate With ERM	RG2.1 Establish and maintain accountability for IT risk management	Who is responsible and accountable in IT risk Management in your organization?
	RG2.2 Co-ordinate IT risk strategy and business risk strategy	Do you consider your IT risk strategy aligned to your business strategy?

Process	**Activity**	**Questionnaire Item**
	RG2.3 Adapt IT risk practices to enterprise risk practices	
	RG2.4 Provide adequate resources for IT risk management	Have you faced resource constraints in your execution of IT risk management in the last financial year?
	RG2.5 Provide independent assurance over IT risk management	Have you performed an external audit of IT or IT risk in the last financial year?
Make Risk-aware Business Decisions	RG3.1 Gain management buy-in for the IT risk analysis approach	Does your management push for your involvement in management of IT Risk?
	RG3.2 Approve IT risk analysis	Does your organization have an IT risk analysis report valid in the current financial year?
	RG3.3 Embed IT risk considerations in strategic business decision making	On a scale of 1 to 5, do you agree that your organization considers IT risk prior to making key business decisions?
	RG3.4 Accept IT risk	Does your mobile lending business maintain documentation of IT risk acceptance decisions?
	RG3.5 Prioritise IT risk response activities	On a scale of 1 to 5, do you agree that your organization prioritises IT risk response activities?
Risk Evaluation Domain		
Collect Data	RE1.1 Establish and maintain a model for data collection	Does your organization maintain a model for the collection, classification and analysis of IT risk data?

Process	Activity	Questionnaire Item
	RE1.2 Collect data on the operating environment	Does the model collect data on external environment or risk events? Does it identify specific risk factors pertinent to digital lending?
	RE1.3 Collect data on risk events	
	RE1.4 Identify risk factors	
Analyze Risk	RE2.1 Define IT risk analysis scope	On a scale of 1 to 5, do you agree that your organization defines its risk analysis scope?
	RE2.2 Estimate IT risk	On a scale of 1 to 5, do you agree that your organization estimates its risk exposure through assessment of likelihood and impact?
	RE2.3 Identify risk response options	On a scale of 1 to 5, do you agree that your organization has a clear understanding of the range of risk response options such as avoid, share, accept and/or seize?
	RE2.4 Perform a peer review of IT risk analysis	On a scale of 1 to 5, do you agree that your organization performs a peer review of its risk analysis before sharing with management for decision making?
Maintain Risk Profile	RE3.1 Map IT resources to business processes	Does your organization have a map of its IT resources to key business processes?
	RE3.2 Determine business criticality of IT resources	On a scale of 1 to 5, do you agree that your organization determines which IT services and IT infrastructure resources are required to sustain the operation of

Process	Activity	Questionnaire Item
		key services and critical business processes?
	RE3.3 Understand IT capabilities	On a scale of 1 to 5, my organization evaluates its IT process capability, skills and knowledge of people, and IT performance outcomes across the spectrum of IT risk.
	RE3.4 Update IT risk scenario components	On a scale of 1 to 5, do you agree that your organization reviews the collection of attributes and values across IT risk scenario components? (e.g., actor, threat type, event, asset/resource, timing)
	RE3.5 Maintain the IT risk register and IT risk map	On a scale of 1 to 5, do you agree that your organization captures its IT risk profile within tools such as an IT risk register and IT risk map?
	RE3.6 Develop IT risk indicators	On a scale of 1 to 5, do you agree that your organization designs metrics or indicators that can point to IT-related events and incidents that can significantly impact the business?
Risk Response Domain		
Articulate Risk	RR1.1 Communicate IT risk analysis results	On a scale of 1 to 5, do you agree that your organization reports its IT risk analysis results in terms and formats useful to support business decisions?
	RR1.2 Report IT risk management activities	On a scale of 1 to 5, do you agree that you consider reporting on IT risk issues

Process	**Activity**	**Questionnaire Item**
	and state of compliance	and status in your organization to be strategic and efficient?
	RR1.3 Interpret independent IT assessment findings	On a scale of 1 to 5, do you agree that your organization is able to review the results and specific findings of objective third parties such as internal audit, quality assurance, external audit, etc.
	RR1.4 Identify IT-related opportunities	On a scale of 1 to 5, do you agree that your organization is able to identify IT-related opportunities that could enable mobile money lending to accept greater risk and enhance growth and return?
Manage Risk	RR2.1 Inventory controls	On a scale of 1 to 5, do you agree that your organization has put in place across risk focus areas, as inventory of controls to manage risk and enable risk to be taken in line with risk appetite and tolerance?
	RR2.2 Monitor operational alignment with risk tolerance thresholds	On a scale of 1 to 5, do you agree that your organization ensures that the mobile lending business line accepts accountability for operating within its individual and portfolio tolerance levels and for embedding monitoring tools into key operating processes?
	RR2.3 Respond to discovered risk exposure and opportunity	On a scale of 1 to 5, do you agree that your organization holds cost/benefit discussions regarding the contribution of

Process	Activity	Questionnaire Item
		new or existing controls towards operating within IT risk tolerance?
	RR2.4 Implement controls	On a scale of 1 to 5, where required, do you agree that your organization takes appropriate steps to ensure the effective deployment of new controls and adjustments to existing controls?
	RR2.5 Report IT risk action plan progress	On a scale of 1 to 5, do you agree that your organization monitors IT risk action plans at all levels to ensure the effectiveness of required actions and determine whether acceptance of residual risk was obtained?
React to Events	RR3.1 Maintain incident response plans	On a scale of 1 to 5, do you agree that your organization prepares for the materialisation of threats through plans that document the specific steps to take when a risk event may cause an operational, developmental and/or strategic business impact?
	RR3.2 Monitor IT risk	Does your organization monitor its IT risk environment?
	RR3.3 Initiate incident response	Does your organization have an incident response plan?
	RR3.4 Communicate lessons learned from risk events	On a scale of 1 to 5, do you agree that your organization examines past adverse events/losses and missed opportunities in order to learn from the events?