OCTAVE-SMALL BASED SECURITY FRAMEWORK FOR MOBILE BANKING AMONG COMMERCIAL BANKS IN THE DEMOCRATIC REPUBLIC OF CONGO

OLIVIER FUMBU MAKEUSA

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF MASTERS OF SCIENCE IN COMPUTER INFORMATION SYSTEMS (MSC. CIS) AT THE KENYA METHODIST UNIVERSITY

NOVEMBER 2020

DECLARATION

This thesis is my original work and has not been presented for a degree or any other award in any other University.

Signature: **Date: November 4, 2020**

OLIVIER FUMBU MAKEUSA

REGISTRATION N^0: CIS-3-1739-1/2015

RECOMMENDATION

This thesis has been submitted for examination with our approval as university supervisors.

Signature: .... Charity Chao**..........** **Date:** 5/11/2020 **..........**

Name: Dr. Chao Mbogo

Kenya Methodist University

Signature: .... **Date: ....**

Name: Adrian Kamotho Njenga

Kenya Methodist University

DEDICATION

I am dedicating this research to my parents, Makeusa Jean and Jeannette Bagomwa, Brothers and Sisters. Thank you all for the encouragement that you have given me.

ACKNOWLEDGEMENT

The following people have been very instrumental and influential to me not only during this research project, but they have provided the support that enabled me to complete my post-graduate studies.

I want to take this opportunity to thank my family, most notably my parents - Mr. Makeusa Kavasohwa Jean & Mrs. Jeannette Mawazo Bagomwa for their undying support and for encouraging me to forge forward to achieve my full potential. Irene Wangui Wanjiru and Saidi Kasongo words can never express my gratitude, Daniel Vihumbira, Kamabu Tasilwiwe Jean-Baptiste Magloire and Mumbere Mughumalewa Jeremy for the constant encouragement and interest in this work and progress. Thank you to Oscar Agastiva, and all my friends and colleagues for their continued support and encouragement during this work.

The faculty of Science and Technology, my supervisors – Dr. Chao Mbogo and Kamotho Njenga, for ensuring that we settled in well and the tireless efforts to make the masters transmission a bearable one. I would also want to thank the Msc. CIS class of 2015 for listening, providing advice, and encouragement for this research from inception to completion.

Finally, the reason for my being - my heavenly Father for giving me life and a continued chance to realise that there is a tomorrow that I can use to better myself.

ABSTRACT

Commercial banks face severe concerns over mobile banking security issues due to substantial monetary losses on customers' accounts. Most customers of commercial banks in the Democratic Republic of Congo have been losing vast amounts of money from their accounts to fraudsters and hackers, who are taking advantage of weak security controls. This has necessitated the present study to be conducted by proposing a mobile banking security framework based on Octave-small approach for commercial banks in the Democratic Republic of Congo. The specific objectives were to; determine critical organisational information influencing the design of a mobile banking security framework for commercial banks in DRC, Construct risks to sensitive assets in information systems that contribute to the implementation of a mobile banking security mechanism for commercial banks in the DRC, analyse infrastructure vulnerabilities prompting the design of mobile banking security framework for commercial banks in DRC, analyse risks prompting the design of mobile banking security framework for commercial banks in DRC, and recommend a security framework for mobile banking among commercial bank in DRC. The research followed a descriptive design, where 227 respondents from the 549 branches of 18 retail banks in the DRC were chosen for the survey. Information was obtained using both questionnaires and interview guides. The questionnaire was used to collect primary data, and the interview guide was used to collect data during interviews. The data were evaluated using a quantitative method to produce descriptive statistics used during inferential analysis to build a model. The study concludes that critical organisational data does have a moderately significant effect on the design of innovative banking security frameworks among reta0il banks operating in the Democratic Republic of Congo; threats to vital M-banking assets moderately impact the effectiveness of mobile banking security frameworks for retail banks operating in the Democratic Republic of Congo, Modest essential and positive effect of infrastructure vulnerabilities significantly impacts on the design of the Mobile Banking Security Framework for the Democratic Republic of Congo retail banks and, Risk reduction has a significant moderate impact on the design of these Mobile Banking Security Framework. The results of the study suggest the detection of sensitive operational information, the identification of risks to strategic assets in information systems, the analysis of network weaknesses and risk analysis, the establishment of a security protection policy and mitigation plan are key determinants of the security framework for retail banks operating in the DRC. The study proposes a four-stage octave framework; identifying critical organizational details for M-Banking; consider the security needs of a valuable asset, creating a risk assessment for each asset, highlighting the key vulnerabilities, and establishing an organizational protection and mitigation strategy in place. The suggested architecture model would include a protection mechanism to secure mobile banking, split into three primary security layers: the client, the contact channel, and the server. The study results would enable commercial banks in the DRC to concentrate on developing and enforcing customer-side protection to reduce this banking service system's risks and vulnerabilities.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS AND ACRONYMS

APPS	-	Applications
CIA	-	Confidentiality, Integrity and Availability
COBIT	-	Control Objectives for Information and related Technology
COSO	-	Committee of Sponsoring Organizations
DRC	-	Democratic Republic of Congo
ICT	-	Information and Communication Technology
IS	-	Information Systems
ISACA	-	Information System Audit and Control Association
ISO	-	International Organization for Standardization
IT	-	Information Technology
M-Banking	-	Mobile Banking
NIST	-	National Institute of Standards and Technology
OCTAVE	-	Operationally Critical Threat, Asset, and Vulnerability Evaluation
PKI	-	Implement mutual authentication using Public Key Infrastructure
SSL	-	Secure Socket Layer
WTLS	-	Encrypt M-Banking using the Wireless Transport Layer Security

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

The world is currently experiencing a rapidly evolving global information system that is able to build a digital economy by creating electronic commerce (e-commerce). The Internet has become a precious business resource for banks due to its almost universal connectivity. (Uvaneswaran et al., 2017). More specifically, Information Communication Technology (ICT) is prominently playing a vital role in growth of the banking sector. This encourages a spread of electronic banking (e-banking) (Troy, 2012) growth with ICT enabling the bank to fundamentally change its functioning. Today E-banking is introducing a new competition phase, due to its unusual, indescribably beautiful and special features: speed, performance, cost reduction and the benefits of the unique opportunities. (Uvaneswaran *et al.*, 2017).

Accordingly, the banking industry is modernizing in the system by employing the state-of-the-art technology and implementing different kinds of e-banking services. Just in the few e-banking facilities available; ATM (Automated Teller Machine), POS (Point of Sale Terminal) Online banking and mobile banking (M-Banking) are featuring prominently. Mobile banking offers many advantages for the consumer and, most notably, allows consumers to conduct their banking transactions where ever, at whatever time and at a reduced rate. (Esmaili *et al.*, 2011). This offers the possibility of providing more functionality for accessing banking and payment systems to current banking customers. In particular, in developing economies, the delivery of banking and payment services are increasingly extended much further to those who have never previously engaged in the formal electronic banking system. (Desisa & Beshah, 2014). Banks, Mobile Network Operator (MNO) and third-party vendors are poised to boost their efficiency from this process. Such incentives have contributed to new entrants entering the market.

While mobile banking provides new opportunities, it is vulnerable to other threats emerging from financial institutions, operators and the financial system. Ashraf (2012) posits that providing internet banking (I-Banking) on a mobile device poses its own security problems, which may weaken the confidence of its customers of their bank. Key among these threats include; fraudulent movement of funds away from their account holder (owner), obtaining Personal identification number (PIN) through social engineering such as phishing and ID theft/imposter, breaching customer's mobile channel and thereby gaining access to all accounts, difficulty to stop suspect transactions, movement of value away from the accountholder to another account outside the accountholders bank, replaying transactions, and repeated transfers from a single account. (Betelhem, 2017). The protection of mobile banking and payments is a core area of concern for customers and financial service providers (Bankable Frontier Associates, 2008). Mobile Financial Service Providers (MFSPs) are also expected to evaluate their risks and to build plans to minimize them on a continuous basis. The transition towards a cautious and modified protection policy needs a proportionate safety structure in order to ensure continuous and successful risk management (Bankable Frontier Associates, 2008).

Risk management approaches and security controls for M-banking can either be quantitative or qualitative according to the risk evaluation and analysis used (Ganthan *et al.*, 2009). Quantitative approaches use empirical outcomes that display the probability of increasing risk factor and its impact on the organizational goals (Mazareanu, 2007).

Qualitative risk assessment analyses and prioritises the influence of established risk factors to determine whether possible risk factors are to be handled (Panda, 2009). In general, qualitative approaches appear to be easier than quantitative ones as they use the protection terminology which is common to non-technological people (Mazareanu, 2007). It makes qualitative risk control approaches a safer alternative in the DRC's banking sector.

Hazard and Operability (HAZOP) research, Failure Mode and Effects Analysis (FMEA) otherwise referred to as Failure Mode and Effects Criticality Analysis (FMECA) and the Government Risk Analysis and Management Method (CRAMM) of United Kingdom (UK) are the most common qualitative risk management approaches (Panda 2009). Some of such qualitative evaluation approaches face significant challenges, including requiring highly qualified professional staff to conduct risk management and interpretation, or labour-intensive. The use of a risk management approach depends on the interpretation and effective use of the system in a specific organizational sense. One process, the Operational Critical Risk, Resource and Vulnerability Evaluation (OCTAVE) system, does not involve highly skilled personnel or heavy financial help (Alberts & Dorofee 2004). It is likely to make OCTAVE the most effective information security risk management tool for use in companies where there are few specialists on computer protection risk management (Alberts & Dorofee, 2001; Panda, 2009). In view of this, OCTAVE, which deals with operational risk in addition to technological threats, can be utilized by the DRC banking sector (Ganthan *et al*., 2009). OCTAVE is structured to build on the skills and knowledge of those inside the company.

The OCTAVE strategy is informed by two aspects: organizational risk and protection standards. Technology is studied primarily in relation to compliance policies, allowing the company to improve its existing protection activities (Alberts & Dorofee, 2004). The OCTAVE strategy makes information-protection choices focused on the threats of secrecy, credibility and availability of sensitive information-related properties. All facets of danger (assets, challenges, weaknesses and operational impact) are taken into consideration in decision-making, allowing an enterprise to balance its security concerns with a realistic defense plan. OCTAVE is self-directed, allowing the company to control the assessment process in order to make information-protection decisions. The assessment is conducted by an interdisciplinary team, termed the Evaluation Group. The team comprises both the parts of the business and the IT Team, as both viewpoints are important in identifying the national, corporate understanding of information protection challenges (Panda, 2009).

Variations in the OCTAVE methodology provide an enterprise with a variety of risk control strategies that are acceptable to the company based on the scale and configuration of the information structures (Panda, 2009). Panda (2009) suggests that OCTAVE-small helps companies to continue to benefit from a database of activities, hazard profiles and risk catalogues. Such catalogs can serve as a guide for commercial banks in the DRC that plan to conduct information technology risk management exercises utilizing simple programming skills (Alberts & Dorofee, 2002). OCTAVE-Small Approach is a comprehensive risk-based strategic information protection evaluation and preparation approach that is a process-driven technique that defines, prioritizes that handles information security threats.

This research therefore reaped from the benefits of the versatility of OCTAVE-small, which can be adapted to specific risk contexts, stability, priorities and the degree of skills required in the banking sector in the DRC (Moyo, 2014). The OCTAVE-small approach to be used in this analysis would be based on four separate processes from the traditional three-phase OCTAVE-small procedure. This is meant to make risk assessment exercise user-friendly and enjoyable for bank employees and, simultaneously achieving the research goals. OCTAVE provides an operational perception of existing information protection threats, offering a realistic overview (baseline) which can be utilized to guide prevention and development efforts. During OCTAVE, the research department carries out exercises to define the cyber protection threats of the enterprise, evaluate the risks to determine goals, and prepare for change in the implementation of an operational progress and risk reduction approach to reduce the danger to the company's sensitive information assets (Albert *et al.*, 2003).

1.2 Statement of the Problem

Despite popularity of mobile banking among commercial banks, protection of customers' information by the respective banks is significantly weak, rendering the client's information vulnerable to outsiders (Betelhem, 2017). There are very serious concerns over security issues, particularly regarding customers' attacks; a recipe to monetary losses on customers' accounts. Specifically, most customers have been losing huge amounts of money from their accounts to hackers, taking advantage of weak security controls. Empirical studies have established losses incurred by customers using M-banking mainly due to weak security controls emanating from banks' ineffective security framework. Further, most M-banking security frameworks are designed in the context of developed economies, limiting their applicability to developed countries. More so, M-banking technology applications are at infancy (Audu, 2018). This fact has denied developing economies such as the Democratic Republic of Congo' the much-needed information for implementing competitive M-banking security frameworks, knowledge gap. The existence of these gaps thus necessitates a need to rationalise the use of an OCTAVE-based security framework for mobile baking among commercial banks in the Democratic Republic of Congo. Moreover, there is a strong pressure on mobile banking application developers to take care of users' privacy as well as the banks security.

1.3 Research Objectives

1.3.1 General Objective

This study's main objective was to assess the current security state of mobile banking and propose a security framework based on the octave-small approach for mobile banking among commercial banks in the Democratic Republic of Congo.

1.3.2 Specific Objectives

The following specific objectives guided the study:

i. To determine critical organizational information influencing the design of a mobile banking security framework for commercial banks in DRC.

ii. To determine threats to information systems critical assets that prompt the design of a mobile banking security framework for commercial banks in DRC

iii. To assess the infrastructure vulnerabilities prompting the design of a mobile banking security framework for commercial banks in DRC

iv. To analyse risks prompting the design of a mobile banking security framework for commercial banks in DRC.

v. To recommend a security framework for mobile banking among commercial bank in DRC

1.4 Research Questions

i. What is the critical organisational information influencing the design of a mobile banking security framework for commercial banks in DRC?

ii. What are the threats to information systems critical assets prompting the design of a mobile banking security framework for commercial banks in DRC?

iii. What are the infrastructure vulnerabilities prompting the design of a mobile banking security framework for commercial banks in DRC?

iv. What are the risks prompting the design of a mobile banking security framework for commercial banks in DRC?

v. What security framework is suitable for the mobile banking among commercial banks in DRC?

1.5 Significance of the Study

Mobile banking services are rapidly being used in the Democratic Republic of Congo and other African countries, based on technologies offered by mobile network operators and retail banks. The significant contribution of this study is to recommend an Octave-small based security framework to support the typical commercial banks in DRC. This would benefit Banks to offer more secured M-Banking services of customers - side to the market, increase the number of customers using the M-Banking technologies, and protects customers from hackers and third-party access to their account information.

To deliver the service, many issues related to the security required to be taken into consideration and some inherent in e-payment systems. How the parties engaged in the transaction handles these security risks may affect mobile banking user's perception of the security of the service. The consumers' knowledge of their responsibility towards the security of the service on their mobile phones could have influenced the use of the service.

1.6 Scope and Focus

This work focused on mobile banking protection concerns. Research work primarily focused on the market use of a banking applications built on bank client's mobile devices. Network security (such as GSM network) or financial infrastructure (including back-end payment processing systems) was not part of the focus of this study.

Work is geographically restricted to applications delivered by financial organizations in the Democratic Republic of Congo (DRC).

1.7 Limitations

Due to the nature of their business, privacy and competitiveness are things that are taken very seriously within the banking sector. As a result, the research encountered challenges when collecting data as banks were not willing to share the information about the information security mechanism they undertake. The research, therefore, was conducted in 18 friendly commercial banks willing to share information relating to security initiatives that they undertake.

CHAPTER TWO

LITERATURE REVIEW

2.1. Introduction

In this chapter is provided an analysis of the literature related to the thesis, as provided by numerous academics, writers, critics and readers. It examines the theoretical literature on security mechanisms that helped to define crucial factors that promote the implementation of a security system for mobile banking in the commercial banks of the Democratic Republic of Congo. This chapter also includes the drawback of the above-mentioned structures, the analysis of the Scientific Evidence, the theoretical holes and, ultimately, the philosophical structure. The theoretical analysis contains all the concepts that tell this research, whilst the empiric one incorporates all the experiments performed by the other scientist and leads this research. The chapter provides a rundown of the evaluations as well as the deficiencies found in previous studies and the methodological structure that has been embraced.

2.2. M-Banking Threats, vulnerabilities and Mitigation Strategies

Security frameworks are known to beneficial to the implementers of the framework in ways such as; reducing the complexity and scope of design and implementation, ability to provide a simple holistic view of a phenomena, improves the decision making process, enables users to see and more importantly, to understand, the flow and evolution of processes and identify any thorny issues that need to be ironed out earlier. Such strategies involve the introduction of Information Security Management Systems (ISMS) in enterprises that stress the goal of formalizing the roles and monitoring of the specified systems. (Moyo, 2014).

Particularly, the whole idea behind having a security framework for mobile banking is to help get the risk balance right. Proper management of mobile devices combined with the challenge of enforcing acceptable usage policy may effectively push organizations into using frameworks. Frameworks would allow organisations to take another look at their policies and update them, thus shrinking them and making them simpler. In the eyes of businesses, mobile devices are the drivers of innovation across a wide range of business processes, while in the eyes of back offices, mainly IT and risk departments, there is a need to be risk-averse (Audu, 2018). Building a framework requires fundamental knowledge on previous frameworks on how they can be enhanced, where to start, and how to proceed and the essential components of the framework. In-depth knowledge is also necessary for aspects such as goals for the framework and its scope (Desisa & Beshah, 2014).

Various frameworks have been developed and used in various domains in the world, and as a result the, definition of a framework would vary depending on the context and domain it operates in. In this respect, Desisa and Beshah (2014) explain that frameworks should be neutral, meaning they should be independent of tools and methodologies. This study reviewed various security frameworks found useful in explaining the proposed security framework for mobile banking. These security frameworks include the; NIST Framework, ISO/EIC Standard security frameworks, Control Objectives for Information and Related Technologies (COBIT), Confidentiality, Integrity & Availability (CIA) Triad for Information Security, Committee of Sponsoring Organizations (COSO), and OCTAVE. Due its flexibility and simplicity, OCTAVE inform this research.

2.2.1 The NIST Framework

Among the commonly used frameworks used is NIST, which is used to provide documentation describing minimum level of requirements for IT security (Hannula, 2018). The NIST framework is based on US information security law. A disadvantage with NIST framework is that it should be used in conjunction with an in-depth information security program (Hannula, 2018); which is lacking in most organizations in developing countries like Kenya. Another weakness is that the NIST framework lack focus on any financial aspects, which makes it not useful across many organizations (Hannula, 2018).

2.2.2 ISO/EIC Standard security frameworks

Some commonly used information security management systems are ISO/EIC Standards such the ISO/EIC 27001:2005 and the ISO/IEC 27005:2008 (Singh & Lilja, 2010). The ISO / EIC 27001:2005 is the UK Standard BS 7799, an international framework for information protection, which has followed a method methodology that develops, applies, runs, tracks, updates, manages and enhances the ISMS, ISO / EIC 27001:2005 Specification follows the Plan-Do-Test-Act (PDCA) paradigm for all its operations, where "Plan" includes the execution of ISMS; "Do" is the execution and management of ISMS; "Test" is the inspection and reassessment of ISMS; and "Act" is the maintenance and enhancement of ISMS. If an entity complies with ISO / IEC 27001:2005, there are assurances that a certain degree of conformity has been reached with each organisation; access protection, connectivity and resource management, enforcement, computer security event management , business stability management , information security strategy, information security agency, equipment management, physical and environmental governance.

ISO / IEC 27002:2005, a widely recognized common standard for cyber management, is an accepted standard for Information Security Management (Singh & Lilja, 2010). This includes guidance for the application of the ISO / IEC 27001:2005 standard. ISO / IEC 270005:2008. The globally agreed framework for computer technology risk management describes a risk management method, comprising contextualization, risk evaluation, risk control, risk recognition, risk communication, and risk analysis and examination. Its method incorporates the PDCA pattern which includes knowledge of the ISO / IEC 27001 which ISO / IEC 27002 codes. Singh and Lilja (2009) postulate that the regulation cannot prioritize controls and calculate the effect of protection improvements.

2.2.3 COBIT (Control Objectives for Information and Related Technologies)

COBIT, which relates to the information protection mechanism, is a risk-oriented IT governance structure established by the Information Management Audit and Control Association (ISACA) focused on the analysis and application of current IT principles and best practices (IT Governance Institute [ITGI], 2007). ITGI (2007) suggests that the system guarantees; IT is compatible with company; IT supports company and maximizes benefits; IT services are utilized sensibly and IT threats are carefully managed. The COBIT system helps managers to cross the difference between management criteria, technological problems and operational risks.

It is an IT governance structure and support toolkit that helps administrators to cross the difference between management criteria, technological challenges and business risks.

Policy formulation within the COBIT system can require significant cooperation with the finance and audit departments. (Rhodes-Ousley, 2013). The COBIT system points out 34 high-level management goals in four company areas. in COBIT, 318 specific control priorities contained in this definition t include knowledge and resource specifications, quality assurance components, quality management, expense and delivery; confidential control components; include efficacy, performance, information reliability, compliance; safety protection components; address security, honesty, and availability.

2.2.4 Committee of Sponsoring Organizations (COSO)

COSO has been a commonly established quality management policy system for SOX enforcement. The advent of mobile apps and associated protection concerns has an effect on the following COSO components: sponsorship commission, risk management, control operations, knowledge and correspondence, and surveillance (Akinleye & Kolawole, 2019)). In the nature of the Control System, mobile devices are a critical component of the control setting and thus ought to be accepted as part of the control process by management within the enterprise. The risk evaluation of the threats related to mobile apps, such as the possibility of data loss, will be identified and evaluated. Control mechanisms ought to be developed to handle the threats to the enterprise raised by the usage of mobile devices (Uwadiae, 2013). Those provide protection of personal data and security options on all electronic apps. Information and collaboration mean that the protection protocols developed for the use of mobile devices continue to be conveyed to the top management. Constant review of the usage and enforcement of mobile devices, including employee-owned devices, with the policy and whether limits on user content are successful.

2.2.5 Confidentiality, Integrity & Availability (CIA) Triad for Information Security

The CIA triad is a traditional, well-known defense strategy formulation paradigm used to define trouble areas and the required cyber management approaches (Chin, 2012). CIA are protection features that help to recognize the effect of such risks; Confidentiality represents the guarantee that knowledge is exchanged only by designated individuals or organizations. Breaches of confidentiality that occur if the details are not treated in an effective way to protect the security of the information involved. This disclosure can occur by hearsay by printing, making a copy, via e-mailing, or the production of records and other details, etc. The classification of the details would assess secrecy and, thus, the necessary protections.

Integrity guarantees that the material is accurate and growing. This guarantees the knowledge can be counted on to be reasonably reliable for its function. The word Integrity is also commonly referenced when discussing Cyber Safety as one of the key safety measures (or lack thereof). Data credibility is not only whether the data is 'right,' nor whether it can be trusted and rely on. For example, creating copies (via e-mailing a file) of a sensitive document violates both security and credibility of the documents. Since, when creating one or more copies, the data is at risk of alteration or adjustment. Availability means that the services responsible for delivering, preserving and transmitting knowledge are available, when possible, to those that require it.

2.2.6 OCTAVE

The OCTAVE risk control strategy includes all risk elements that involve properties, risks and weaknesses (Alberts & Dorofee, 2001). This is a monitoring system to assess the extent of vulnerability and to prepare protections against information attacks. The system describes a technique to help organisations mitigate vulnerability to potential risks, determine the possible effects of an assault, and cope with active attacks. OCTAVE is built to draw on the skills and knowledge of individuals inside the company. The first move is to build threat profiles based on the relative danger they pose. The OCTAVE-specific vulnerability evaluation approach is a systematic tool for evaluating and examining cyber security threats depending on the nature of cyber infrastructure assets that is suitable for the usage of internal corporate tools to conduct threat / application risk assessment that review. (Storms, 2003).

Numerous reports on OCTAVE as an information technology risk assessment method note the benefits of employing this strategy in organisations with different sizes, irrespective of the technological expertise of the staff (Panda, 2009). The critical value of OCTAVE is that it is participatory and self-directed (Panda, 2009). As OCTAVE is used, various actors have the ability to effectively engage in risk evaluation and appraisal practices, thus strengthening their decision-making process for the security and control of information system tools. Unlike the traditional technology-focused appraisal, which focuses on technical danger and focuses on operational problems, OCTAVE focuses on organizational danger and focuses on political, practice-related concerns. It is a versatile assessment that can be customized to most organisations. When implementing OCTAVE, a small team of people from the Organizational (or Business) Departments and the IIT Department works together to fulfill the protection requirements of the enterprise.

OCTAVE offers an operational perception of emerging cyber protection threats, a realistic overview or a benchmark that may be utilized to guide prevention and development efforts (Alberts et al., 2003). Through OCTAVE, the department determines the cyber security threats of the enterprise, analyzes the hazards and evaluate goals and action strategies by creating a defense policy for operational development and risk reduction measures to reduce the danger to the company's sensitive assets.

OCTAVE is structured around these three main elements, which enable operational personnel to obtain a detailed image of the cyber protection needs of the company. Those involve creating asset-based threat maps, finding network flaws, and designing compliance policies and plans. Creating Asset-Based Risk Profiles is an operational evaluation in which the research department decides what is important to the enterprise (information-related properties) and what is actually being done to secure such properties. The team then identifies the items that are most essential to the enterprise (sensitive items) and defines the protection criteria for each sensitive object. Finally, it defines risks to each vital asset and generates a vulnerability profile for that asset. Defining system weaknesses is an information architecture appraisal, where the research department explores network access mechanisms, defining clusters of information security elements relevant to each essential object. The team must then assess the degree to which each class of the item is immune to network attacks. Throughout the implementation of the Safety Strategies and Policies, the research department determines threats to the essential assets of the company and discusses what to do with them. The department shall establish a security policy for the enterprise and contingency strategies to mitigate the threats to sensitive infrastructure, centered on an overview of the information obtained.

The OCTAVE approach has been described as the most suitable framework for this reason as it is a process-driven approach that defines, prioritizes and handles information management vulnerabilities within the information structure of the enterprise (Panda, 2009 OCTAVE is structured to provide the company with full knowledge on cyber protection risk control (Alberts & Dorofee, 2002). The OCTAVE risk assessment mechanism is self-directed as it allows individuals inside the same company to function collaboratively and take accountability for the organization's protection policy (Tiwari, 2010), result that this research aims and accomplish.

Varieties of the OCTAVE approach provide an enterprise with a range of risk control approaches relevant to the entity based on the scale and structure of the information systems (Panda, 2009). Alberts and Dorofee (2002) claim that when applying the OCTAVE-small risk management model, the company continues to benefit from a database of activities, hazard assessments and vulnerability catalogues. Such catalogs may serve as a guide for commercial banks in the DRC who plan to participate in information security risk reduction activities utilizing workers with specific computer skills.

OCTAVE-S has the same three main phases; develop asset-based threat profiles; define network vulnerabilities; and security strategy. Organisational knowledge is defined and used to identify vulnerability profiles for three to five sensitive information-related properties during the development of asset-based vulnerability profiles. It includes the detection of corporate knowledge and the development of hazard profiles. The research department determines the organization's critical information-related properties, establishes a series of effect measurement requirements, and describes the existing condition of the organization's protection activities. While designing threat profiles, the research department chooses three or five sensitive knowledge assets and determines the protection criteria and threat profiles for those items.

While detecting network weaknesses, a high-level evaluation of the systems and technology-related activities is conducted by the research department to optimize the vulnerability profiles. This was accompanied by a study of the critical assets network infrastructure by the research team evaluating access paths in networks that serve critical assets and assessing how effectively their technology-related mechanisms secure those assets. During the formulation of security policies and schedules, the threats to vital assets are analyzed and an organizational safety and risk reduction approach is developed. The research unit analyses all operational threats for effects and, optionally, for danger detection and interpretation. We would also create prevention measures and contingency methods; in this case the department would establish an operational safety and risk control approach focused on best standards.

This analysis would take advantage of the versatility of OCTAVE-small, which can be tailored to match the particular information structures of banking sector in the Democratic Republic of Congo in terms of risk environments, stability, priorities and the degree of skills required. The OCTAVE-small approach used in this study focused on four phases: identification of sensitive operational details, identification of critical asset information systems risks, analysis of network weaknesses, risk analysis and implementation of M-Banking protection and mitigation strategies for commercial banks in the DRC. It is meant to make the practice of risk reduction user-friendly and enjoyable for bank employees and, at the same time, to accomplish study objectives as in Table 2.1.

Table 2 1:

Sample Mapping of outputs to the OCTAVE-small method

Output	**Implementation in the OCTAVE-small method**
Critical assets for CISs	Process 1: Data was gathered through an asset identification and inspection checklist and interview of two key users of CISs in each school. This included members of the collaborative teams who eventually identified critical assets.
Organisational security practice to safeguard critical assets and areas of concern	Process 1: Data gathered through interviews of system users including collaborative team members
Security requirements for critical assets	Process 2: Users of CISs defined security requirements for their important assets. The collaborative team used this information to establish the security requirements for the school critical assets.
Current security practices	Process 2: Users of information systems assets contributed their views on security practices currently being used by each school. Two users completed a simple security checklist. Follow-up discussions on key issues were made. Collaborative teams consolidated security practices
Threats to critical assets	Process 2: Collaborative teams inspected critical information systems assets to identify threats. Users of CISs were observed using assets and also interviewed on areas of concern. The collaborative teams used these areas of concern as input to create a threat profile for each critical asset in tabular form
Current organisational vulnerabilities	Process 3: Users of CISs contributed their views on missing or inadequate security practices in the schools (organisational vulnerabilities).

Key components	Process 3: Collaborative teams identified key components of the computing infrastructure. The teams used the critical assets and the threats to select key components.
Technical vulnerabilities	Process 3: Each collaborative team evaluated each key component using vulnerability evaluation tools like Windows Defender and antivirus. Manual checks for vulnerabilities on the network and computers were performed
Risks to critical assets	Process 4: Each collaborative team identified the potential impact of the threats to critical assets. A list of risks was produced in tabular form.
Protection strategy	Process 4: Collaborative teams developed possible protection strategy for organisational security improvement. The strategy was based on organisational and technological vulnerability information.
Risk mitigation plans	Process 4: Collaborative teams developed risk mitigation plans to reduce the risks in CISs critical assets. Each team selected mitigation actions based on the organisational and technological information security risks identified throughout the evaluation process.

Source: Moyo (2014)

2.2.7 Limitation of the frameworks

The frameworks reviewed were particularly oriented on the usage and regulation of mobile devices in the business climate. Whilst the components specified are, to a certain degree, specific to mobile devices as used by M-banking customers. That is because the inherent risks to a company are the same as to a customer (such as ransomware, system loss), although the effect may, of course, be different. Okay, according to Chin (2012). The COBIT system comprises of 210 different regulations, several of which do not relate to defined risks associated with customers’ mobile devices.

Primary characteristic of a framework is that it should be easy to use and reduce the time spent to solve problems. The goal of this paper was to identify a customized system focused on risk profiles and, eventually, the analysis should contribute to a customized protection framework for M-baking in among retail banks operating in the Democratic Republic of Congo.

2.3. Theoretical Framework

The study reviewed the Willie Sutton Theory of Cybersecurity by Alan Cohen as well as the Cybersecurity Information Sharing Theory.

2.3.1 The Willie Sutton Theory of Cybersecurity

The Willie Sutton Theory originates from response to interview by Willie Sutton on a bank robber who recorded a statement indicating that he robbed banks because that was where the money was attributed to (Bamrara, 2015). Thus, bank servers and storage devices that manage and safeguard the vast bulk of a company's or government agency's data are targeted because of the data in them. The theory suggests a three-step process for better segmentation of high-value assets through; comprehensively understand your computer environment, creating a segmentation model that ring-fences high-value assets, and create a zero-trust model for high-value assets

Under comprehensively understand your computer environment, the bank cannot secure what one cannot see. Better security requires a comprehensive mapping of all workloads and network flows. Moreover, this is not a one-time activity, but rather a continuous requirement (Bamrara, 2015). Security managers must move rapidly toward continuous monitoring of compute and network activity. When creating a segmentation model that ring-fences high-value assets, all data is important and not all information assets are created equal. A breach of the cell phone numbers of key employees would be an uncomfortable exposure. Access to top customer accounts and passwords would be dramatically more severe. Security teams must first put the most focus on locking down critical assets from more general compute resources. To create a zero-trust model for high-value assets, traditional network segmentation models are fairly coarse-grain and create an enormous attack surface for bad actors. Traditional network segmentation schema including; firewall blacklists, and VLANs/zones are difficult to maintain in dynamic environments and leave too much attack surface available to hackers. More-focused whitelist models and encryption within and across the data center and cloud can support a zero-trust model for server-to-server communications (Bamrara, 2015).

2.3.2 The Cybersecurity Information Sharing Theory

The Cybersecurity Information Sharing Theory suggests that m-banking administrators must explain what information sharing is and how it works to address real privacy concerns overcoming lack of trust (Pala & Zhuang, 2019). Information sharing between organization need to flow rapidly and in both directions between the government and the private sector. It provides that the private sector should be provided with legal protection, freedom of information, and regulatory protections for sharing information. It advocates for broad information sharing to ensure banks have the information they need to prevent threats, risks and attacks on customer’s information.

2.4. Empirical Literature Review

This segment presents a review of some particularly related works in Mobile Banking security frameworks for the commercial banks. The study analyses and identifies gaps that exist in previous works. Audu (2018) researched on technology adoption in the DRC revealed that perceptions of the user have a high statistical significance for their intention to do their shopping online. Nevertheless, as the connection between understanding and desire to buy online is moderated by familiarity, it was notice that there is a disparity between people with previous online shopping experience and those without online shopping experience.

The study by Betelhem (2017) on appraising the conceptual protection system for the authentication of moving banking key and exchanging of messages protocols between Ethiopian banks, came up with an approach that will strengthen the mobile banking security. They identified that their main concern was on the authentication keys of the application, including the message exchange process. Eventually, a modern architecture has been established that will allow the banking industry to ensure the protection of M-banking key authentication and exchanging of messages. The Betelhem (2017) study advises that the URL inspection method on the customer side should be further improved for its accuracy and reliability, and rigorous testing should be carried out, and work should also address usability problems in the future. It depends on what represents an appropriate degree of protection and on the trade-off between accessibility and protection.

Janulevicius (2016) study assessment on the information protection risk analysis approach for virtualized environments, concluded that the implementation of a virtualization application risk analysis offers ample evidence to modify and enforce security measures to ensure an optimal degree of protection. The study showed that, while several methods exist, they do not have a coherent protection research comparison environment. In 2016, Rovito carried out a research introducing a standardized model specific to supply chains that would direct consumers through current risk testing methods and expose details on network flaws as well as incentives for decision-makers to participate. Suh a model, adaptable to a range of structures and capable of identifying non-obvious points of risk, can be utilized by network engineers to express device awareness and have a comprehensive view of the dynamic supply chain. In fact, the common model allows the customer to draw up a collection of vulnerabilities and associated solutions and to convey details on weaknesses in the supply chain to judgement-makers and other stakeholders.

A research by Moyo (2014) undertaken among secondary schools on computerized information systems showed that learners were vital assets; continuous appraisal points, financial records , personal details for educators, personalized program applications, server machines, and telecommunications equipment used for networking. The key risks to these vital assets included allowed and unauthorized device users, ransomware, machine failures, access routes, and program incompatibilities. The dangers raised by such attacks is exacerbated by the unavailability of the properties of essential information networks, the lack of data privacy and confidentiality. It has contributed to a lack of profitability and revenue and harm to the credibility of the institution. Physical defense was the only type of safety system imposed by secondary schools. In order to minimize outstanding threats, the study has equipped school administrators and consumers in identifying, designing and applying specific security and prevention techniques in accordance with their information structures, financial capacities, and ability rates.

This report by Moyo (2014) indicated that secondary schools have vital CIS properties that need to be safeguarded; secondary school administrators are dedicated to cyber protection to protect their CIS but lack the necessary expertise and experience to achieve; secondary schools will strive to adopt good operational management policies and technological measures to mitigate security vulnerabilities in their CIS. This study further suggested that secondary schools delete all sensitive devices from open-source school networks, encrypt all essential information, password-protect all critical information devices and educate all users of personal security information systems.

Douramanis carried out an analysis in (2014) in which the findings showed that there were several separate cyber challenges, but we did not find particular threats that threatened our institution mostly as Supervisory Control and Data Acquisition (SCADA) network center. Therefore, the listed risks can be deemed important to any network configuration. The report states that there are security attacks that may threaten the SCADA network core. Such attacks differ based on the form they use, along with the internet communication protocol they use to transmit their payload. However, we could not find some kind of attacks or hosts that directly threaten their VNs as they imitate the SCADA network.

The study by Padyab et al. (2014) utilized Genre Based Method (GBM) into a lightweight risk assessment method, OCTAVE Allegro. It was suggested that GBM could be used in parallel with OCTAVE Allegro during the information asset mapping with the help of producers and users of information (PUI) or their representatives. PUI entities participate in a social debate to scrutinize genres in which they transfer information with the help of supported tools like diagonal matrix and genre worksheet. Further on, identified information assets are fed into OCTAVE Allegro for further risk assessment. The result shows that GBM's supported tools and guidelines can identify channels of communication where there is a potential leakage. This study, therefore, suggests that GBM can facilitate the enumeration of information assets through channels of communications or genres.

This research by Padyab et al. (2014) indicates that GBM provides the investigator with instructions about how to continue recognizing intelligence properties embedded in corporate contact genres. During this analysis, it was observed that information and expertise properties are often defined as genders are classified, since genders are not tied to particular institutions or procedures. It was also disclosed that GBM is capable of detecting intelligence properties that are buried deep inside corporate structures and day-to-day job routines. The study showed that the organized method of GBM would enable the researcher to define knowledge assets (facilitator) in a versatile manner. Therefore, GBM can; classify information assets in a standardized way, maintain a market strategy context integrated into the risk management method, enhance the identity of information asset owners.

Research by Taubenberger (2014) suggests an approach to resolving risk detection mistakes using compliance specifications and business process models. Safety specifications reflect the protection needs of the company and decide that any flaw is a safety risk to the business. Safety specifications for information assets are analyzed in the framework of the business process model in order to assess how protection mechanisms are properly applied and managed. Systems, staff and functional aspects of business operations, as well as IT systems, are included in the health condition evaluation phase and are tested in three phases. Second, there are two best-practice solutions to the standardized method. First, the quality of the potential estimate is related to the best-practice risk-assessment method applicable to a variety of real-world scenarios within an insurance firm. Third, the capacity to define danger more effectively with the use of company procedures and protection criteria is evaluated in a quasi-experiment by security practitioners. This work indicates that risk management approaches will profit from the clear evaluation of safety criteria in the company sense during risk detection, in order to address deficiencies in the recognition of errors and to include a protection criterion.

Shaaban's (2014) report on improving governance of information security in developed countries and especially in Zanzibar proposed a semiotic mechanism model for improving governance of information security. The workflow model was also used to test the new cyber management culture system. The semiotic assessment of the cyber management culture system has enabled the development of a comprehensive structure and integrated social and technological approaches on the basis of the corporate semiotics method. The semiotic paradigm for information protection culture has made it easier to identify answers to issues encountered in certain structures across structures. That was clear by the usage of contextual approaches in various levels.

Ochuko (2012) worked on e-banking organizational risk evaluation showed that the structure and assessment instruments produced strong forecasts for risk analysis and inference in these frameworks. Therefore, the findings obtained can be deemed encouraging and valuable for both the introduction of the E-banking program and potential researchers in this area.

A research by Ashraf (2012) showed that certain specific trends appeared when coping with protection dimensions of mobile banking in the sense of mobile apps and applications. Unless such concerns are not adequately handled by security controls and interventions, the underlying risks may threaten the secrecy, credibility and availability of mobile technology properties. Mobile security assets that require defense include mobile computers, mobile apps, and private details. In this study, eight threats have been identified. These risks may be classified in the following ways: consumers, computers, apps and records, and governance. Based on this categorization and interviews with experts in the area of banking and IT protection, a M-Banking Safety Framework has been created that can be used to identify security controls and interventions, to carry out risk analyses for M-banking in the sense of mobile apps and mobile apps, or to plan an audit fieldwork.

A study by Bankable Frontier Associates (2008) concludes that a proportionate regulatory framework ensures that an organisation maintains active risk management in its mobile banking. The study advises for the establishment of a robust risk system for both banks and non-banks. This further advises that mFSPs create a robust, proportionate structure under which appropriate and continuous monitoring of mFSPs can take place. It means that sufficient consideration is given to detecting, tracking and managing mobile channel threats while offering ample room for risk-appropriate technologies that may be omitted where existing, static security requirements occur.

2.5. Research gaps

The review of the existing literature showed that the security of mobile banking had been widely researched in developed and emerging economies. However, there is limited research concerning the security of mobile banking technology in both bank and customer sides, for the developing economy such as DRC. Therefore, research is required to address this gap by customizing a security framework by considering banking business security requirements as it locks the gap.

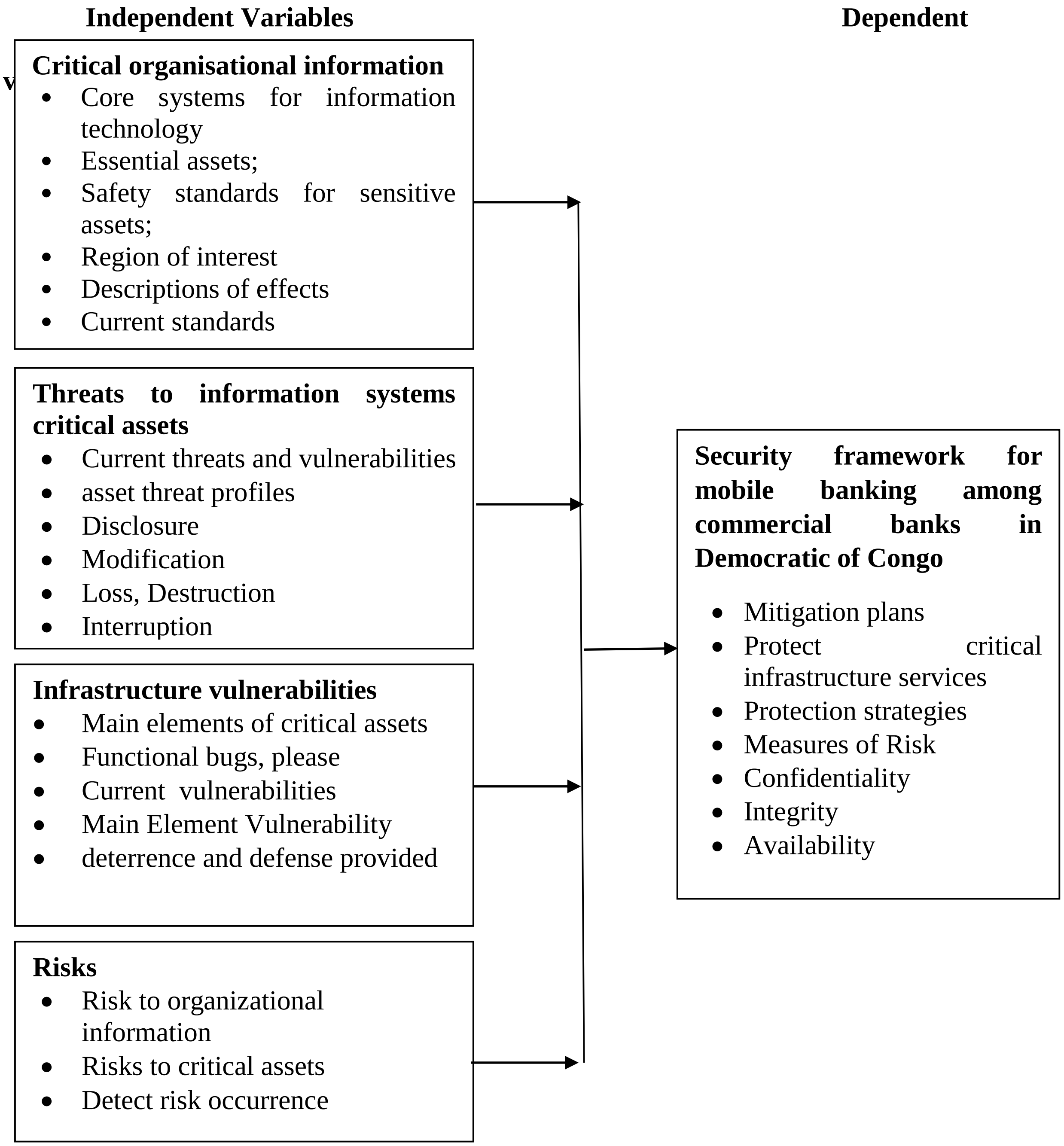
2.6. Conceptual framework

Following the evaluation of qualitative approaches, this research was justified in choosing the OCTAVE risk management process. The OCTAVE method presents a simplified alternative from which different organizations, depending on the skills of the team may have, can carry out risk assessment and evaluation exercises. OCTAVE covers all risk components (assets, risks, and vulnerabilities) and, as a result, an entity obtains adequate data to completely match its information security policy with risk management, unlike traditional approaches. (Alberts & Dorofee, 2001; Panda, 2009).

This means that OCTAVE is a risk management and appraisal approach focused on organizational threats and protection standards, where computer infrastructure is analyzed primarily in relation to information security activities (Panda, 2009). The key aspects of the OCTAVE-s are: recognition of sensitive operational details, detection of risks to essential information networks, review of network weaknesses and risk assessments, and establishment of a protection policy and mitigation strategy. The detection of sensitive operational details, the identification of risks to essential assets in information networks, the examination of network weaknesses and risk analysis, and the implementation of a data management policy and contingency plan are independent variables, whereas the security framework for retail banks in the DRC is a dependent variable.

Figure 2.1:

Conceptual Framework


Independent Variables
Dependent
v
Critical organisational information
• Core systems for information technology
• Essential assets;
• Safety standards for sensitive assets;
• Region of interest
• Descriptions of effects
• Current standards
Threats to information systems critical assets
• Current threats and vulnerabilities
• asset threat profiles
• Disclosure
• Modification
• Loss, Destruction
• Interruption
Infrastructure vulnerabilities
• Main elements of critical assets
• Functional bugs, please
• Current vulnerabilities
• Main Element Vulnerability
• deterrence and defense provided
Risks
• Risk to organizational information
• Risks to critical assets
• Detect risk occurrence
Security framework for mobile banking among commercial banks in Democratic of Congo
• Mitigation plans
• Protect critical infrastructure services
• Protection strategies
• Measures of Risk
• Confidentiality
• Integrity
• Availability

Source: Researcher (2019)

CHAPTER THREE

RESEARCH METHODOLOGY

The methodology for the thesis is discussed in this section. This includes the development of research, target population, sampling methods and techniques, methods and methods for data collection, validation and accuracy checks and proposed techniques for data analysis, including ethical considerations.

3.1 Research Design

Gupta and Rangi (2016) clarified that a study framework was required to help the researcher build a plan for collection of data, data assessment and analytics. As a master plan, the study model sets out the tools and techniques needed to optimize data collection and efficient evaluation. It also lists all the activities involved in carrying out the work at hand.

The research design, which is inclusive of the preparation process and the plan for information gathering, analysis and evaluation, is a clear strategy setting out the plans and procedures for data collection, and its use review and other activities relating to study development. Study design discusses the issues; why the research is being undertaken, the intent of the analysis while the analysis is being undertaken, where the research would be conducted. Where evidence is accessible and its kind, which technique is used to gather data, which strategy of collecting data, which pattern of sampling and which type of data reporting is viable (Gupta & Rangi, 2014). The analysis used a concise research method to define, evaluate and assess the critical factors required to establish a mobile banking protection system for commercial banks in the DRC. The concise research model was used to raise knowledge and resolve current issues (manifestation) of the M-banking protection network among retails banks in the DRC. This concept is used to collect knowledge regarding behaviours, beliefs, behaviour and other potential behaviours. Descriptive techniques were used to gather and address questions regarding mobile banking protection system details and answers question on; who was available to provide the data, what data was to be collected, where the data was to be collected, why the data was needed and how the data was to be collected. Six Ws (who, what, where, where, why, way) are used for descriptive research (Gupta & Rangi, 2014).

3.2 Study Population

The current survey determines the entire study population with the most suitable characteristics, with sufficient details on the system for M-banking protection, based on the concept of target population of Mugenda and Mugenda (2008), which refers to issues related with general study findings and which have specific measurable characteristics. Across all mobile banking activities, IT managers were well placed and versed on issues pertaining to M-Banking. The present research thus established the target population as 549 retails bank branch 'IT administration in the Democratic Republic of the Congo of. There were usually 549 retail banking branches in the DRC. Each branch then presented its IT director / manager as their respondents. Thus, the research targeted the 549 IT branch managers across DRC. The choice of the branches, instead of the headquarters, was informed by the different challenges faced branches in different region. That is branches from the sane bank encounter differ in challenges due to their locations and the beliefs as well behaviors of the local community (where their clients come from) differences.

3.3 Sampling Procedures and Techniques

The sample size has taken into account the desired heterogeneity and data quality (Creswell, 2104). Kothari (2012) describes a survey as chosen interviewees reflecting the whole community. A properly designed sampling frame helps a researcher without worry about inaccurate entries that reflect the elements related to the excluded community to take care of the identified target population. The sample frame should be complete, appropriate, accurate and suitable. A representative sample from the survey system was chosen, which would represent the community as far as possible.

Krejcie *and* Morgan (1970) formula $\boldsymbol{s = \chi 2NP\ (1- P)\ /\ [d^2\ (N -1) + \chi 2P\ (1- P)]}$ was adopted for establishing the sample size as 227 respondents from a target population of 549. In formula;

s = required sample size.

$\chi 2$ = the table value of chi-square for 1 degree of freedom at the desired confidence level

(3.841).

N = the population size.

P = the population proportion (assumed to be .50 since this would provide the maximum sample size).

d = the degree of accuracy expressed as a proportion (.05).

Given the sample size = $s = \chi 2NP\ (1- P)\ /\ [d^2\ (N -1) + \chi 2P\ (1- P)]$

Then s = [3.841 x 549 x 0.5 (1 – 0.5)]/ [0.05 x0.05 (270-1) + 3.841 x 0.5(1- 0.5)]

= (3.841 x 549 x 0.5 x 0.5)/ [(0.05 x0.05 x 548) + (3.841 x 0.5 x 0.5)]

= 527.18/ (1.38+ 0.96)

= 527.18/ (2.34)

= 226.23

≈ 227

Therefore, the sample size was 227 respondents from the 549 branches.

The analysis just used in its proportionate stratified to assess each bank's sample size expressed all the branches of these retails banks multiplied by total sample as a fraction of the target population, The research then established a sample interval for each bank, consisting of all branches for that commercial bank, after identifying the branches required in each bank. The research obtained the sampling interval for each bank to be used for the identification of respondents (participating branches) from that bank. For branches, the sampling interval was determined as number of branches divided by the all respondents needed by the commercial bank. Subsequently, the participants were chosen randomly using a basic random sampling method and directed by the sampling interval.

3.4 Data Collection Methods and Procedures

The thesis aimed to develop the methods for the processing of its data and the correct techniques to be used in the collection of data. It is important to collect reliable and sufficient data from the analysis. The study looked at the compilation of primary source data using a structured questionnaire. A standardized questionnaire includes only closed questions allowing respondents to select answers from pre-defined choices and to give respondents the freedom to answer questions. The questionnaire was conducted using the drop and pick process. In some cases, the researcher has been asked to explain the questions.

3.4.1 Data Collection Methods

The present research used a standardized questionnaire (only closed-ended questions) to gather data from primary sources. The questions in the questionnaire were focused on the goals of the analysis. It should be remembered that closed-ended questions are sufficient to provide alternate answers from which respondents can chose. However, questionnaires are acceptable for literate respondents and are therefore useful for the collection of data needed in a concise analysis. It should also be remembered that the concise analysis allowed data to be obtained from respondents efficiently, conveniently and ideally in a non-threatening manner. The data used in the questionnaire was calculated using the Likert scale of 5 (1-5) points.

3.5.2 Data Collection Procedures

When all the data as accessed, the study then undertook pilot tests on the testing instrument to assess efficacy and validity. The pre-test respondents were not permitted to engage in the data collection. Following a positive analysis of the testing method, the researcher went into intensive data collection. Effective data collecting included the implementation of the questionnaire, where the researcher received as much help as necessary so that the respondents could address the questions correctly. On receipt of the completed questionnaire, the researchers first checked the entries and then explained the problems resulting from the filling of the questionnaire or the unresolved issues. As the data was collected from an existing institutional institution, the researcher first requested approval to collect data from the management of the institutions, upon which the researcher and the related individuals rendered agreements as to when and how the data were to be obtained.

3.5 Validity and Reliability

Prior to research starting intensive data collection, the instrument itself was checked for validity and reliability. Such checks are important in order to develop and maintain the reliability and integrity of the instruments used for data collection in the field of science. Pretesting, in addition, reveals the shortcomings of the software and allows for their analysis and enhancement by editing and, thus, guarantees that the method is suitable for the collection of the required data and the planned timeline. This is at this period that the researcher found some possible issues associated with the method. (Kvale, 2007). Pre-testing was also used to determine the validity of the goals of the analysis as it assessed the comprehensibility of the survey tool.

3.6.1 Validity

Kothari (2012) suggests that the validity of that same instrument is an indicator of the degree to which it determines the requirements of the sample and thus guarantees that the method is relevant and effective for the data collection of the analysis. Upon the basis of these claims, the present thesis checked the quality of the questionnaire in order to assess its consistency and significance using the material validity check. The validity check tests the degree to which the questionnaire data gathered will be unique to the operational success and strategic management metrics within the financial institution region of the DRC. The check was carried out by sending a questionnaire to two independent experts who measured the relevance of the questionnaire. Such specialists were IT security professional and the other college supervisors. The IT protection specialist was charged with helping to evaluate the questionnaire and decide if the collection of things in it will correctly quantify the results of the octave methodology focused on the M-Banking Safety System Model for retail Banks in the Democratic Republic of Congo, whilst the supervisor evaluated the questionnaire with a view to defining the definition to be calculated by the questionnaire.

3.6.2 Reliability

This is accuracy and reliability of scores over time, tests to the extent that the entire system is error-free and would result in a consistent instrument result. Reliability tests are conducted to identify critical study issues, including: data sources, data collection methods, data collection time and tool bias (Kvale 2007). In the analysis, 5 interviewees were provided with a questionnaire for a period of one (1) week to answer the question. Upon collecting the responses, the researcher enhanced the questionnaire by changing elements which were not reliable.

The research tested the quality of the questionnaire using an independent Cronbach alpha testing methodology. The internal accuracy of the data gathered was calculated for the time being by the similarity of elements in the questionnaire identified as the Cronbach alpha. The value for alpha varies from 0 to 1. In social science, the instrument is graded as insufficient internal reliability or clearly unreliable if the alpha coefficient would be less than 0.7. Nonetheless, the Cronbach alpha value larger than or equivalent to 0.7 implies better accuracy if the reassessment of reliability will otherwise be regarded.

3.7 Proposed data analysis techniques and procedure

Upon efficient data analysis, the researcher reviewed the data for omission and contract errors. The questionnaires with incorrect or inaccurate responses were removed, and the researcher instead started an examination of the right questionnaire. Throughout the study, the researcher first identified the data and encoded the same data accordingly. The encoded details was evaluated using a quantitative research method for the related descriptive statistics. The research was carried out on the basis of the test aims, insulating every test variable to define the characteristics for this variable and the association to the dependent variable. Descriptive statistics, comprising average, frequency, percentage and standard deviation, were developed, describing the properties of the respective research variables and focusing on test objectives. The findings of the data collection were seen in the tables and statistics and also in the narratives.

Third, the inferential research conducted to generate inferential statistics to assess if there was some association between the Independent Variables (IVs) and the Dependent Variable (DVs) tests. Correlation review for each IV to assess if there is a meaningful association was carried out first. Utilising multiple regression analysis, the analysis sought to create a model for estimating the security system for M-banking in terms of predictor IVs as in the model;

$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + e$………………………………………………… (i)

In which case;

Y = Security framework for mobile banking among commercial banks in Democratic of Congo

X_1 = Critical organisational information

X_2 = Threats to information systems critical assets

X_3 = Infrastructure vulnerabilities

X_4 = risks

β_0 is a constant. This is the value of Y when each of β_1, β_2, β_3, and β_4 is 0.

β_1, β_2, β_3, and β_4 are the regression coefficients representing the change induced by X_1, X_2, X_3 and X_4

e = error term

The predictor IVs are the study variables; critical organisational information, threats to information systems critical assets, infrastructure vulnerabilities, and risks.

During the calculation of the sample model, the study checks predictions using Analysis of variance (ANOVA) process. The research used the Pearson product test at a significance point of 0.05 (p-value < = .05). The research conducted various analyses using the regression findings to assess the importance of the experiment at the 5 % confidence point (0.05 significance point). The present thesis was aided in the review of data using SPSS (Statistics Program for Social Sciences) software version 22.0.

3.8 Ethical Considerations

In attempting to satisfy ethical concerns, the researcher first requested a letter to enable a report to be undertaken by the Kenya Methodist University Study Board. When performing the analysis, the report maintained the confidentiality and reliability of the data gathered by the respondents. In order to maintain confidentiality and secrecy, the researcher kept the data in safe custody. In fact, the researcher cautioned the respondents not to include their names on the questionnaire in order to prevent disclosing who received the details. With each questionnaire, the researcher attached a letter asking the respondent to engage in the data collection, a gesture of respect to the respondents, as well as a procedure to ensure informed consent to participate in the analysis.

3.9 Evaluation Protocol

The study adopted a structured questionnaire to collect data for the study. The operationalization of the study tool is captured in the Table 3.1.

Table 3.1:

Evaluation Protocol

Question	Type	Description	Scale	Measure	Analysis
Qn1	Demographic	Respondents gender	Nominal	Labels 1 and 2 for male and female respectively	Quantitative to produce frequency
Qn2	Demographic	Period worked with the Bank	Nominal	Label	Quantitative to produce frequency
Qn3	Demographic	Highest level of academic qualifications	Nominal	Labels	Quantitative to produce frequency
Qn4	Demographic	Period in the current position	Nominal	Labels	Quantitative to produce frequency
Qn5	Demographic	Period using school information systems assets	Nominal	Labels	Quantitative to produce frequency
Qn6	Demographic	Frequency of receiving formal training in using computer infromation systems	Nominal	Labels	Quantitative to produce frequency
Qn7	Demographic	familiarity with information security risk management	Ordinal	Likert Scale	Quantitative to produce frequency
Qn8	Independent variable	List of the key information technology systems	Nominal	Narrative Analysis	Qualitative (based on themes – thematic analysis)
Qn9	Independent variable	Critical assets in your organisation	Nominal	Narrative Analysis	Qualitative (based on themes – thematic analysis)
Qn10	Independent variable	Main security requirements for critical assets	Nominal	Narrative Analysis	Qualitative (based on themes – thematic analysis)

Qn11	Independent variable	Areas of concern of the CIS	Nominal	Narrative Analysis	Qualitative (based on themes – thematic analysis)
Qn12	Independent variable	Impact descriptions of organisation’s CIS	Nominal	Narrative Analysis	Qualitative (based on themes – thematic analysis)
Qn 13	Independent variable	Current security practices of your CIS	Nominal	Narrative Analysis	Qualitative (based on themes – thematic analysis)
Qn14	Independent variable	Occurrence of threats in the organisation’s CIS	Ordinal	Likert Scale (1-5)	Quantitative to produce descriptive
Qn15	Independent variable	current threats and vulnerabilities CIS critical assets	Nominal	Narrative Analysis	Qualitative (based on themes – thematic analysis)
Qn16	Independent variable	Asset threat profiles	Nominal	Narrative Analysis	Qualitative (based on themes – thematic analysis)
Qn17	Independent variables	Integrity of information system assets	Ordinal	Likert Scale (1-5)	Quantitative to produce descriptive
Qn18	Independent variable	Threats to information systems critical assets	Rate	Likert Scale Index ratio	• Quantitative to produce descriptive • Regressions
Qn19	Independent variable	key components for critical infrastructure assets	Nominal	Narrative Analysis	Qualitative (based on themes – thematic analysis)
Qn20	Independent variable	Technical vulnerabilities on the infrastructure assets	Nominal	Narrative Analysis	Qualitative (based on themes – thematic analysis)
Qn21	Independent variable	current technological vulnerabilities	Nominal	Narrative Analysis	Qualitative (based on themes – thematic analysis)

Qn22	Independent variable	vulnerabilities for key components	Nominal	Narrative Analysis	Qualitative (based on themes – thematic analysis)
Qn23	Independent variables	deterrence and (or) defense provided	Ordinal	Likert Scale Index ratio	Quantitative to produce descriptive
Qn24	Independent variables	Risks to CIS	Nominal	Narrative Analysis	Qualitative (based on themes – thematic analysis)
Qn25	Independent variables	Risks to critical assets	Nominal	Narrative Analysis	Qualitative (based on themes – thematic analysis)
Qn26	Independent variables	CISs risk related issues	Rate	Likert Scale Index ratio	• Quantitative to produce descriptive • Regressions
Qn27	Independent variables	Proneness of CIS assets to risk	Rate	Likert Scale Index ratio	• Quantitative to produce descriptive • Regressions
Qn28	Independent variables	Effect on availability of organisational information	Ordinal	Likert Scale Index ratio	Quantitative to produce descriptive
Qn29	Independent variables	Risk in terms of monetary loss associated with mobile banking	Nominal	Narrative Analysis	Qualitative (based on themes – thematic analysis)
Qn30	Independent variables	Risk in terms of harm to mobile banking customers records caused misuse	Nominal	Narrative Analysis	Qualitative (based on themes – thematic analysis)
Qn31	Independent variables	Risk of loss of privacy because of information collected about customers when using mobile banking	Nominal	Narrative Analysis	Qualitative (based on themes – thematic analysis)

Qn32	Independent variables	Risk rating on mobile banking	Nominal	Narrative Analysis	Qualitative (based on themes – thematic analysis)
Qn33	Independent variables	anyone’s email address used to send emails to their contacts without their consent	Nominal	Narrative Analysis	Qualitative (based on themes – thematic analysis)
Qn34	Independent variables	Information security breaches	Ordinal	Likert Scale Index ratio	Quantitative to produce descriptive
Qn35	Independent variables	Vulnerabilities on customer mobile banking systems	Ordinal	Likert Scale Index ratio	Quantitative to produce descriptive
Qn36	Dependent variable	Status of mobile banking security framework among commercial banks in Democratic of Congo	Rate	Likert Scale Index ratio	• Quantitative to produce descriptive • Regressions

CHAPTER FOUR

DATA ANALYSIS AND DISCUSSION

4.1 Introduction

This article explains the outcomes of the review of the data collected from the sample report, as well as the conclusions and comments on these conclusions. In this chapter, the chapter's key contents are the review of the reliability and validity checks, the answer rate of the sample, and the demographic statistics. It is accompanied by comprehensive figures on quantitative data processing, as outlined in the chapter with an inferential approach for creating a paradigm that is generalized from the community as a whole. The findings are portrayed in a pictorial way utilizing statistics and tables for ease of understanding and a description of the tests.

4.1.1 Reliability Tests

Reliability is the indicator of the degree to which the artifacts of the research instruments are error free and in turn yield reliable results. The two factors underpinning the principle of durability are the quality of the instrument over time and the intrinsic accuracy (homogeneity) of the calculation of the products. The present study sought to collect data from 27 respondents from three the main microfinance institutions, which use mobile banking applications. However, the response rate 20(70.07%) responded. The data collection for reliability tests took a period of two week, which gave the study a bearing on the average length of time the actual data collection would have taken. The results obtained from the pilot testing of staff questionnaire produced a reliability coefficient (Cronbach’s Alpha) of 0.51, indicating a near inconsistency. Accordingly, the study removed five indictors were contributing the inconsistency. These were; “Our bank has never experienced any disclosure of customers mobile information”, “Staff are aware about Information System threats”, “Congestion”, “Improper disposal”, and “customer reports”. After removal of these items, another reliability test was run to produce the results table 4.1.

Table 4.1:

Reliability Test Results

Study Variables	**Cronbach's Alpha**
Security framework for mobile banking among commercial banks in Democratic of Congo	0.466
Critical organisational information	0.779
Threats to information systems critical assets	0.518
Infrastructure vulnerabilities	0.823
Risks	0.515
Cronbach's Alpha = 0.719, N = 5	

Source: Research Data (2019)

The findings revealed ta Cronbach alpha coefficient of 0.719 that was beyond the 0.7 limit indicated by Kothari (2012). Kothari suggests that as Cronbach's Alpha reaches 0.7, the device becomes strongly accurate. Because Cronbach's Alpha reaches 0.7, this indicates a strong degree of continuity between the elements of the device. The results in Table 4.1 indicate that the internal accuracy was 0.719, suggesting good reliability of the analysis variables. Each of the variables; essential operational knowledge (0.779), Infrastructure weaknesses (0.823) had internal consistency > 0.7, suggesting a very strong consistency of research variables, whereas challenges to sensitive infrastructure in the information networks (0.518) and hazards (0.515) were reasonably consistent. The protection system for M-banking among commercial banks in the Democratic Republic of Congo (0.466) was weak in quality. The analysis was thus found to have a very strong accuracy and to be suitable for the calculation of all test variables in order to obtain reliable and valid findings.

4.1.2 Validity Tests

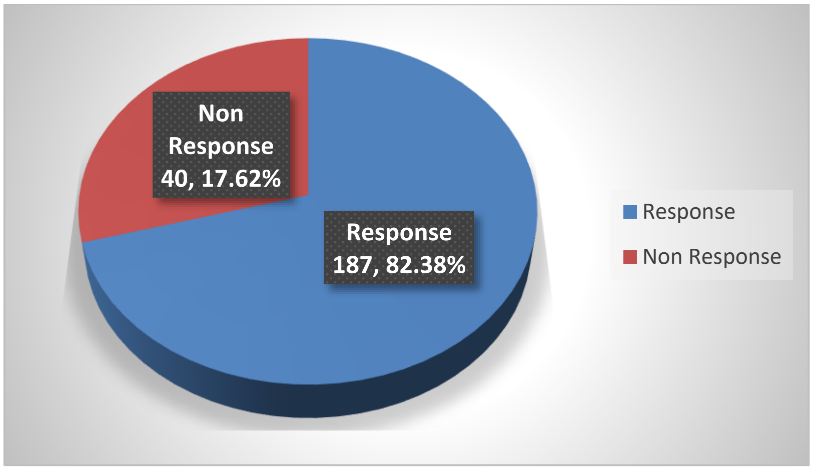
The experts evaluated the tool and made recommendations accordingly. They both concurred that the research instruments (Questionnaire) would measure the desired objective and could be used in the security framework. They however, suggested changes to be incorporated in the questionnaire, which were effectively done. The questionnaire was reviewed through restructuring and reduction of the questions. Various changes made on the research tool after the content analysis by professionals.

4.2 Response Rate

The survey tool was administered to 227 respondents, 187 of whom replied accounting for 82.38%. Nonetheless, 17.62 % did not respond. Anyone who addressed the questionnaire addressed all of the questions very honestly. The intensity of response can be seen in Figure 4.1.

Figure 4.1:

Analysis by Response Rate



Source: Research data (2019)

Figure 4.1 shows a 187(82.38%) response rate, which was good enough to produce accurate since it exceeded 69%. A response rate 82.38% was considered to produce reliable and valid results based on the suggestions by Mugenda and Mugenda (2008). Mugenda and Mugenda (2008) implied that the response rate ranging from 50% to 59% is appropriate, whereas the response ranging within 60% and 69% is ideal and the response rate of more than 69% is quite strong and desirable for reliable tests. Based on this argument, the actual response of 82.38% for this analysis was quite strong, because it was beyond 69%. Although the results were interpreted as suggesting an excellent response rate, some respondents were too busy to respond to the study and could have explained why 17.62% did not respond.

4.3 Respondents’ Socio-Demographic Information

The questionnaire examined participant’s personal characteristics covering the socio-demographic details in the context of sex, age brackets, the educational attainment and the span of experience of ICT protection.

4.3.1 Gender

The participants indicated their gender and the results of analysis shown in table 4.2.

Table 4.2:

Participants Gender

Gender	Frequency	Percent
Gender as Male	175	93.58%
Gender as Female	12	6.42%
Total	187	100.00%

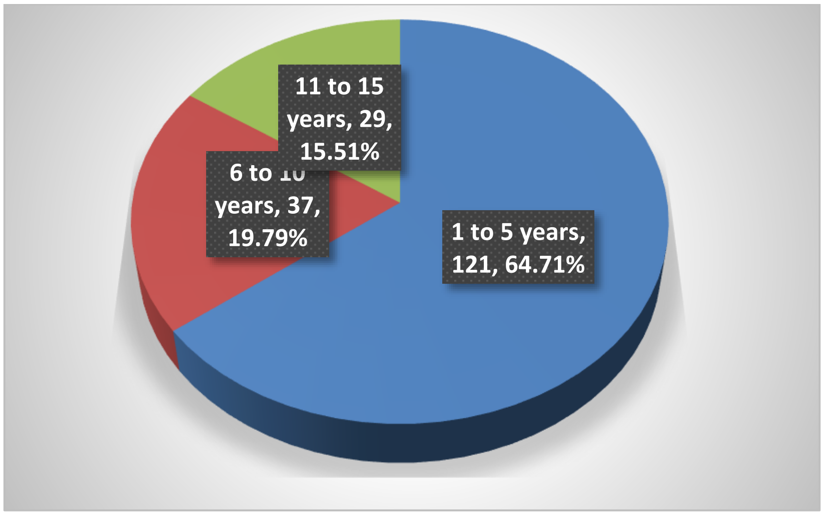
Source: Research data (2019)

The results show that out 187 respondents, 175(93.58%) were male while the remaining 12(6.42%) were female. These results showed that they a case of gender discrepancy in the field. This was indication that most of the employees of banks in DRC were men

4.3.2 Time worked with the Bank

Figure 4.2:

Time worked with the bank



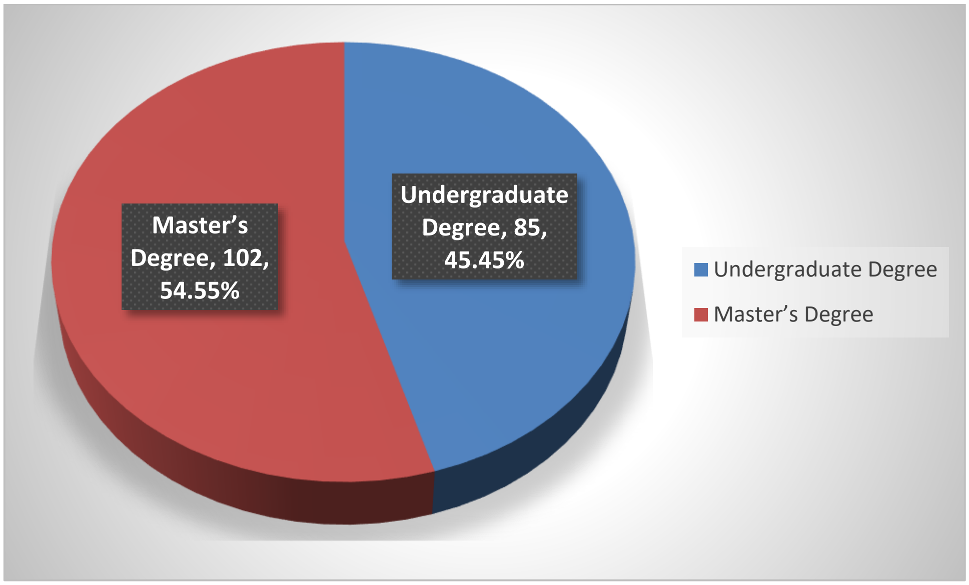
Source: Research data (2019)

The findings reveal that there is a plural majority of 121(64.71%) of the participants had been with bank for between one (1) and five (5) years followed by 37(19.79%) who indicated that they had been in their banks for between six (6) to 10 years and finally 29 (15.51%) who showed that they had between 11 and 15 years with their organisations.

4.3.3 Highest level of academic qualifications

Figure 4.3:

Highest level of academic qualification



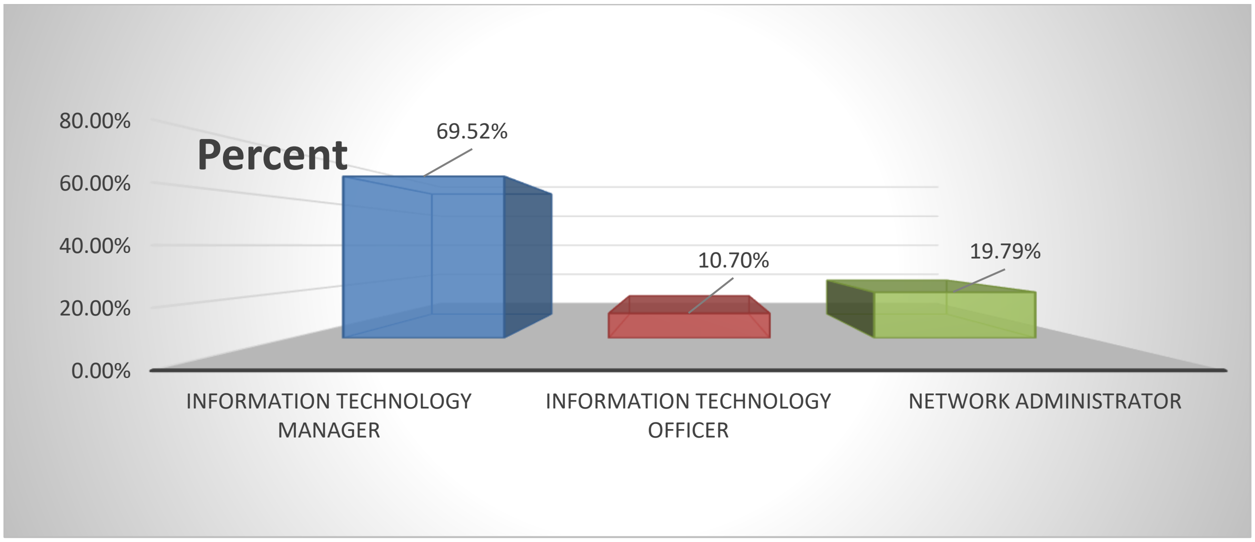
Source: Research data (2019)

Based on the results, it was shown that there were two (2) categories of academic qualifications observed, where a majority of 102(54.55%) of the respondents said they had Masters Degrees and 85 (45.45%) said they were university graduates, with a first degree in university.

4.3.4 Current position in the bank

Figure 4.4:

Current Position in the bank

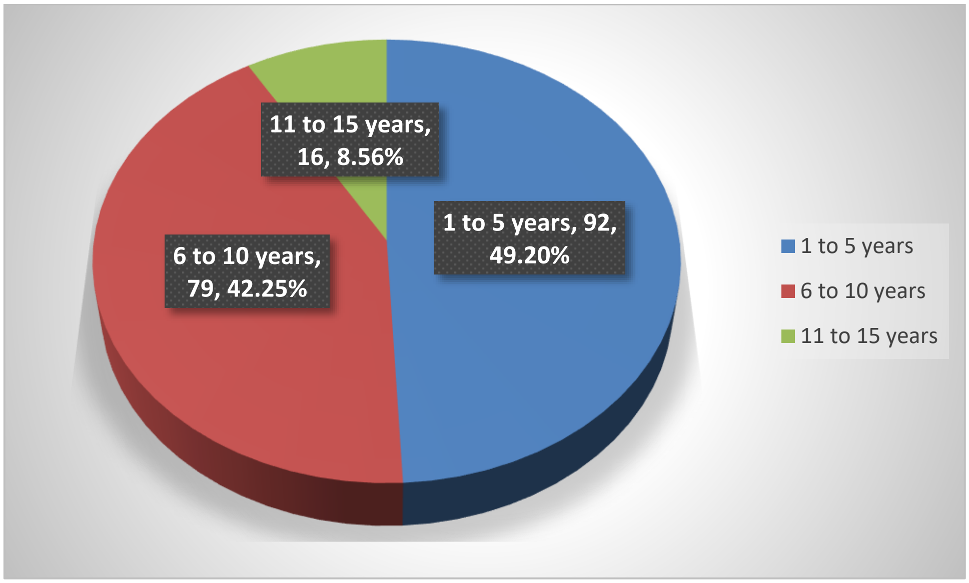


The participants were asked to provide their current positions held in the bank and a popular majority of 69.52% specified that they were IT managers as 19.79% showed that they were Network administrators and 10.70% indicated that they were information technology officers as shown in figure 4.5.

4.3.5 Time been in the position

Figure 4.5:

Time been in the position



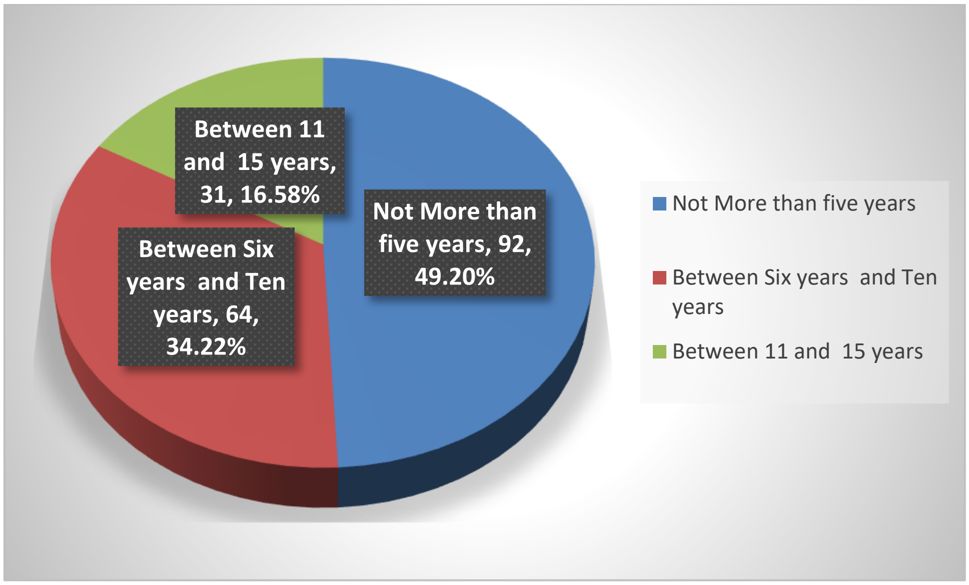
Source: Research data (2019)

The respondents also requested to indicated the time they had held their current position, where most of them, 92(49.20 %) indicated they had been in their current positions for between 1 and 5 years. As 79(42.25%) indicated that they had been in those positions for between 6 and 10 years, 16(8.56%) showed that they had been in those positions for between 11 and 15 years as shown in the figure 4.6.

4.3.6 Time been using bank information systems assets

Figure 4.6:

Time been using bank information systems assets



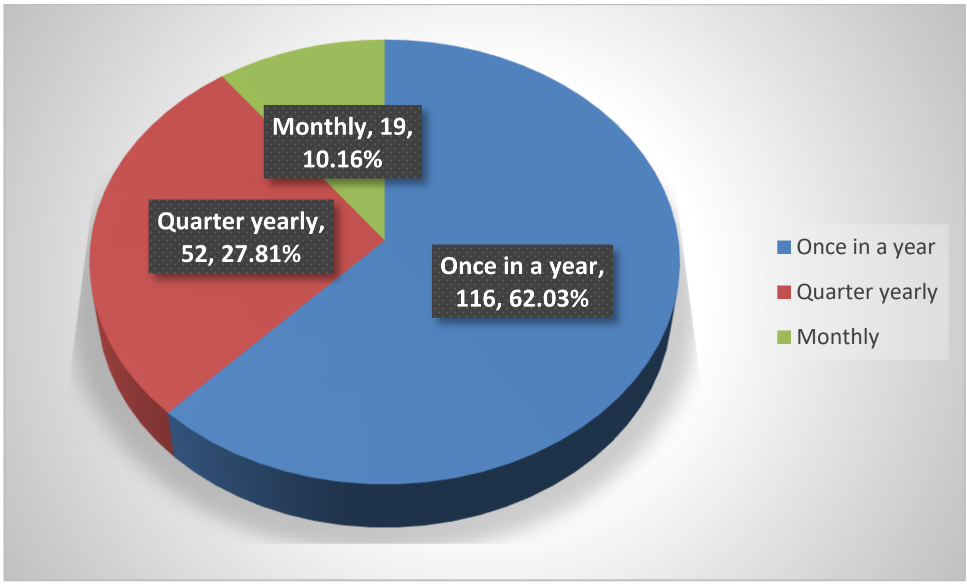
Source: Research data (2019)

Nearly half of the participants, 92 (49.20 per cent), suggested that they utilized tools of banking information systems. For not more than five years while 64(34.22%) indicated they used these for between six to ten years and 31(16.58% indicated they used these system for between 11 to 15 years as shown in figure 7.

4.3.7 Frequency of receiving formal training in using computer information systems

Figure 4.7:

Frequency of receiving formal training in using computer information systems



.

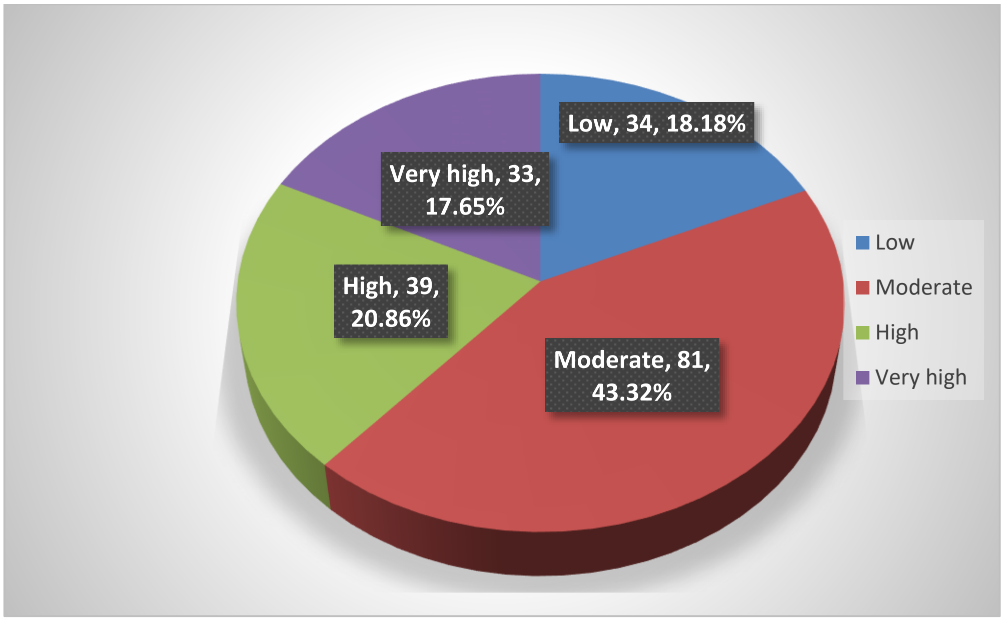
Source: Research data (2019)

The respondents were also asked to indicate the frequency of receiving formal training in using computer information systems. While a majority of 116(62.03%) indicated they did it once a year, 52(27.81%) showed that they did it on a quarter yearly basis while 19(10.16%) showed that they did monthly trainings as shown in figure 8.

4.3.8 Level of familiarity with information security risk management

Figure 4.8:

Level of familiarity with information security risk management



Source: Research data (2019)

Concerning the level of familiarity security risk management in IT, 81(43.52%) indicated they had a moderate level of familiarity. While 39(20.86%) indicated their level of familiarity was high, another 33(17.65%) indicated that it was very high and the other 34(18.18% indicated they had a low familiarity level as displayed in figure 4.8.

4.4 Descriptive Analysis

The research evaluated the characteristics of the target-driven variable using the answers collected using the survey tool, where the questions were calculated using the 5-point (1 – 5) Likert scale; 1, 2, 3, 4, and 5 for “strongly disagree”,, “disagree”,” neutral”, “agree”, and “strongly agree” respectively. The analysis provided an average (M) and a standard deviation (SD) of the tests that were partially mediated to 1 to 1.8, above 1.8 to 2.6, above 2.6 to 3.4, above 3.4 to 4.2 and 4.2 to 5.0 for “strongly disagree”,, “disagree”,” neutral”, “agree”, and “strongly agree” respectively

4.4.1 Critical organisational information

The study’s first objective was to determine the influence of critical organizational information on the design of a mobile banking security framework for commercial banks in DRC. Using results from the checklist, the study found that there was a wide range of critical organisational information that was required for mobile banking. This information was kept by the banks for the purpose of building and maintaining the customers’ accounts and for ensuring effectiveness and efficiency of the transactions taking place. The critical organisational information as informed by the respondents include all that was need for customer mobile database. The majority of the respondents, 156(83.42%) showed that in their banks there was for critical information pertaining to account opening (Consumer enrollment with an intention to using m-banking facilities). In the results obtained a majority of 171 showed it (91.44%) that there was need for information on balance inquiry. As all of them, 187(100.00%) showed that other critical information was on customers database and for credits and withdrawals (depositing and withdrawing respectively 140(74.87%) showed that funds transfer information was critical and a majority of 96(51.34%) showed that information on bill payment was critical. According to these results, a majority of 109(58.29%) showed that alerts was critical information. While 62(33.16%) showed that information on airtime purchase was critical, 31(16.58%)

indicated that loan application information was critical and showed that 78(41.71%) another critical information was on loans disbursed.

Table 4.3:

Analysis by Critical Organisation Information

Critical Organisation Information	**M**	**SD**
Key information technology systems are properly protected in our bank	2.43	0.89
The banks critical assets are have never been attacked by any threats	3.07	1.11
Security requirements for critical assets are properly followed in our bank	2.97	1.36
Areas of concern are not subjected to any threat	2.35	1.28
Threats to impact descriptions have never affected the mobile banking	3.78	0.72
Threats to current security practices are always mitigated	3.89	0.45
Average Critical Organisation Information	**3.08**	**0.97**

Source: Research data (2019)

Participants showed neutrality on the claim that information provided on the critical organizational information as influencing the development of mobile security framework (M=3.08, SD= 0.97) while they disagreed that key information technology systems were properly protected in their bank (M=2.43, SD=0.89) and exposed neutrality on the proclamation that areas of concern were not subject to any threat (M= 2.35, SD=1.28). Together with displaying neutrality on assumptions that banks critical assets were never attacked by any threats (M= 3.07, SD=1.11) and the participants exhibited neutrality on the statement that security requirements for critical assets were properly followed in their banks (M= 2.97, SD=1.36). The respondents agreed that threats to impact descriptions had never affected the mobile banking (M=3.78, SD=0.72) and further agreed that threats to current security practices were always mitigated (3.89, SD=0.45).

During the interpretation of the results in table 4.3, the study used; “not at all” for “strongly disagree”; “low” for “disagree”; “moderate” for “neutral”; “high” for “agree” and “very high” for “strongly agree”. Premised on those findings, the analysis showed that crucial organizational information had a modest impact on construction of mobile banking security framework among commercial banks in DRC. The key information technology systems were not properly protected in their bank and the areas of concern were subjected to some threats. The results show that the banks’ critical assets were sometimes attacked by any threats and at other time, it was not attacked. Further, security requirements for critical assets were moderately properly followed in their banks. The study found that threats to impact descriptions had never affected the mobile banking. However, threats to current security practices were always mitigated.

The participants indicated the level of occurrence of the threats in their computer information system. The scale below was used to measure the level of occurrence of the threats; “Not Applicable” =1; “Low” = 2; “Medium” =3; “High” =4; “Very High” =5. On obtaining the M) and SD, the statistics were moderated to be interpreted as; 1.0 to 1.8 for “Not Applicable”; “Above 1.8 to 2.6” for “Low”; Above 2.6 to 3.4 for “Medium” ; Above 3.4 to 4.2 for “High”; and Above 4.2 to 5.0 for “Very High”.

Table 4.4:

Level of Occurrence of Threats

Level of Occurrence of Threats	M	SD
Decommissioning	3.91	0.72
Lack of awareness	3.65	1.00
User permission fatigue	3.51	1.08
No privacy protection best practice	3.58	0.83
Phishing	4.24	0.86
Spyware	3.44	1.27
Spoofing attacks	4.04	0.64
Diallerware	3.57	0.82
Vulnerabilities leading to malware installation	3.37	1.25
Data leakage	2.03	0.81
Unintentional data disclosure	3.47	0.86
Surveillance	2.72	1.10
Application malfunction	3.09	1.31
Encryption weaknesses	2.76	1.25
Weak app. Distributor authentication mechanism	2.47	1.59
Weak sandboxing	3.22	1.27
Addressed risk of mismanagement adequately	3.29	1.26
Average Level of Occurrence of Threats	3.32	1.05

Source: Research data (2019)

As illustrated in table 4.6 earlier in this thread, the participants exhibited the threats as moderately affected mobile banking systems in the banks (M = 3.32, SD = 1.05). Thus, they were able to classify the threats by their level of occurrence where the levels were low, medium, high and very high. Each of data leakage (M = 2.03, SD = 0.81), weak application distributor authentication mechanism (M = 2.47, SD = 1.59) was shown to have had a low influence. Also, each of; surveillance (M=2.72, SD = 1.10), encryption weaknesses (M = 2.76, SD = 1.25), application malfunction (M = 3.09, SD = 1.31), weak sandboxing (M = 3.22, SD = 1.27), addressing risk of threat mismanagement adequately

(M = 3.29, SD = 1.26) and vulnerabilities leading to malware installation (M = 3.37, SD = 1.25) was shown to have had medium level of occurrence. Each of the variables; spyware (M = 3.44, SD = 1.27), unintentional data disclosure (M = 3.47, SD = 1.26), user permission fatigue (M = 3.51, SD = 1.08), lack of awareness (M = 3.65, SD = 1.00), no privacy protection best practice (M = 3.58, SD = 0.83), diallerware (M = 3.57, SD = 0.82), decommissioning (M = 3.83, SD = 0.83), congestion (M = 3.92, SD = 0.79) and spoofing attacks (M = 4.04, SD = 0.64) was said to have had high level of occurrence. The respondents showed that phishing (M = 4.24, SD = 0.86) had a very high level of occurrence as shown by the respondents in the table above.

We interpreted the findings in Table 4.4 and found a slight effect on critical information on mobile banking systems in banks. The data leakage and the authentication mechanism of the weak application distributor have low impacts. Improper disposal, monitoring, encryption weaknesses, application failure, poor sandboxing, spyware and risk mismanagement unless moderately affected mobile banking systems are adequately addressed by the organization. On the other hand, unintended disclosure of information, user permission fatigue, malware installation vulnerabilities, lack of awareness, best practices in the field of privacy protection, diallerware, decommissioning, congestion and spoofing attacks on mobile banking systems that have been severely affected. Mobile banking networks are primarily targeted at phishing.

4.4.2 Threats to information systems critical assets

The study assessed the second objective to identify risks to sensitive assets in the information systems that will contribute to the implementation of a mobile banking protection structure for commercial banks in the DRC and obtained results in Table 4.5.

Table 4.5:

Threats to Information Systems Critical Assets

Effects of threats to Information Systems Critical Assets	**M**	**SD**
Current threats and vulnerabilities affect the customers' mobile data in way	3.03	1.09
Our bank has never experienced any disclosure of customers mobile information	3.60	1.30
There has never been any modification customers mobile information in our bank	2.61	1.47
There has never been any occurrence of interruption on customers mobile information	1.32	0.57
Average status of Threats to Information Critical Assets	**2.64**	**1.11**

Source: Research data (2019)

The findings reveal that the participants suggested a neutral status of threats to critical information systems in the bank (M = 2.64, SD = 1.11). They were neutral that current threats and vulnerabilities do not affect the customers' mobile data in anyway (M = 3.03, SD = 1.09). They approved that their banks had never experienced any disclosure of customers mobile information (M = 3.60, SD = 1.30) and that they neutral on the assertion that there had never been any modification customers mobile information in our bank (M=2.61, SD=1.47). They strongly disagreed that there had never been any occurrence of interruption on customers mobile information (M=1.32, SD=0.57).

Table 4.6:

Exposure to Threats to Information Systems Critical Assets

Exposure to threats to information systems critical assets	**M**	**SD**
T experts have restricted exposure to the framework.	1.32	0.47
Data transmission between the bank and the client is quite reliable in that only weak encryption is in place.	1.41	0.49
The operating structures, e.g. the payroll program, contain many updates.	2.45	1.35
The firewall is installed correctly; the domains are not restricted.	2.90	1.47
All service identities used are active in the MS Active Directory.	2.59	1.44
Appropriate disaster management and business continuity documents are given.	2.75	1.45
Data and knowledge have been kept safely	2.95	1.22
Confidential information is securely stored	2.75	0.92
Average exposure to threats to information systems critical assets	**2.39**	**1.10**

Source: Research data (2019)

The respondents also gave their opinion on exposure to threats to information systems critical assets and disagreed that the threats influenced information system critical assets (M = 2.39 SD = 1.10); strongly disagreeing with the notion that IT specialist had restricted exposure to the framework (M=1.33, SD=0.47) and that data transmission between the bank and the client was quite reliable in that weak encryption is in place (M=1.41, SD=0.49). They disagreed that the operating structures had several patches (M=2.45, SD=1.35). They were neutral on all other indicators including; use of administrative accounts (M=2.59, SD=1.54); security and confidentiality of information (M=2.75, SD=0.92); appropriateness of disaster recovery (M=2.75, SD= 1.45); proper configuration of the firewall (M=2.90, SD=1.75) and security of documents (M= 2.95, SD=1.22).

So, there was a moderate occurrence of threats including interruptions on customer mobile information with their banks having reported any loss or destruction of the information at some point. Current threats and vulnerabilities moderately affected customers’ mobile data in some way. Banks had never experienced any disclosure or modification to the customer’s mobile information.

In regards to this, the threats lowly influenced information system critical assets. IT specialists were not having restricted access and the data transfer between the bank and client was insecure as only the weak encryption used in the framework. Operating structure had several patches lowly influenced the information system critical assets. The information system critical assets were moderately influenced by; active administrative accounts; secure storage of confidential information; presence of appropriate disaster recovery and business continuity documentation; properly configured firewall; staff well aware of IS threats and secure storage of information.

4.4.3 Infrastructure vulnerabilities

The third objective was to analyze infrastructure vulnerabilities prompting the design of mobile banking security framework for commercial banks in DRC.

Table 4.7:

Mitigation of Infrastructure Vulnerabilities

Mitigating infrastructure vulnerabilities	M	SD
Key components for critical assets are protected against vulnerabilities in our bank	2.88	1.00
Technical vulnerabilities on customer mobile data are properly mitigated	3.08	0.78
Current technological vulnerabilities do not affect customer mobile data	3.05	0.91
vulnerabilities for key customer mobile data components are always diverted	3.34	0.97
Our bank provides a very high level of deterrence and (or) defense provided on customer mobile data	2.97	0.91
Average mitigating infrastructure vulnerabilities	3.06	0.92

Source: Research data (2019)

The respondents were neutral on infrastructure vulnerabilities were mitigated (M=3.06, SD=0.92). All indicators observed were neutral and these including; key components for critical assets were protected against vulnerabilities in their bank (M=2.88, SD=1.00); technical vulnerabilities on customer mobile data were properly mitigated (M=3.08, SD=0.78); current technological vulnerabilities did not affect customer mobile data (M=3.05, SD= 0.91); vulnerabilities for key customer mobile data components were always diverted (M=3..34, SD= 0.97) and finally that their banks provides a very high level of deterrence and (or) defense provided on customer mobile data (M=2.97, SD= 0.91).

With this in mind, the infrastructure vulnerabilities moderately prompted the design of the mobile banking security framework. The key components were moderately protected against vulnerabilities while technical vulnerabilities were moderately mitigated. Current technologies partially affected customer mobile data, vulnerabilities for key customer mobile data components were moderately diverted and the banks provided average level of deterrence on customer mobile data. A collection of vulnerabilities and associated approaches is important, and policy makers and other stakeholders will illustrate vulnerabilities information.

4.4.4 Risks

The fourth objective was to analyze risks prompting the design of mobile banking security framework for commercial banks in DRC. The study first assed the mitigation on risks among these banks.

Table 4.8:

Risks to CIS

Risks	**M**	**SD**
Risk to organizational customer mobile banking information is always mitigated	3.03	0.75
There are no risks to critical customer mobile banking assets	2.75	0.62
Our banks information always detects risk occurrence on customer mobile banking	2.34	1.26
Average Risks	**2.71**	**0.87**

Source: Research data (2019)

Despite the participants exhibiting neutral on the proclamation that risks on mobile banking were mitigated (M = 2.71, SD = 0.87), they disagreed that their banks information always detects risk occurrence on customer mobile banking (M = 2.34, SD = 1.26). Neutral was exhibited on the claim that Risk to organizational customer mobile banking information is always mitigated (M=3.03, SD=0.75) and that there are no risks to critical customer mobile banking assets (M=2.75, SD=0.62).

Respondents also provided details on the level on which CIS assets were prone to risk.

Table 4.9:

Level of CIS assets proneness to risks

Level of CIS assets proneness to risks	**M**	**SD**
Computers especially those used for online banking.	1.91	0.28
Records program	1.81	0.84
Customers’ accounts	1.53	0.64
Customers reports	1.72	1.18
Back-up disks stored the strong room	3.16	1.60
Company records	3.23	1.20
Company information	3.60	1.42
Router and the network equipment	3.30	1.39
Average Level of effect of CIS assets prone to risks	**2.53**	**1.07**

Source: Research data (2019)

On risks, the respondents also gave information on the level to which CIS assets were prone to risk. They showed that CIS assets were lowly prone to risk (M=2.53, SD=1.07). Indicators such as customer’s accounts (M=1.53, SD=0.64), records program (M=1.81, SD=0.84) and customers reports (M=1.72 SD=1.18) were observed not to have been influenced according to the respondents. Computers especially those used for online banking (M=1.91, SD=0.28) were said to have been lowly influenced. Back-up disks stored the strong room (M=3.16, SD=1.60) and company records (3.23, SD=1.20), and router and the network equipment (M=3.30, SD=1.39) were moderately influenced. However, company information (M=3.60, SD=1.42) highly influenced according to the respondents.

In this regard, risks had moderate influence in the design of mobile banking security framework. The banks information lowly detects risk occurrence on customer mobile banking. However, risks to organizational customer mobile banking information is moderately mitigated and no risks were observed to critical mobile banking assets.

From the results obtained in table 4.9 CIS assets are lowly prone to risks. Customer accounts, records program and customer reports were not prone to any risk. Computers especially those used for online banking were lowly influenced by the risks while back-up disks stored the strong room and company records were moderately influenced by the risks. On the other hand, router and the network equipment and company information was highly impacted by the risks.

4.4.5 Mobile banking security framework among commercial banks in Democratic Republic of Congo

The study analysed the dependent variable; mobile banking security framework among commercial banks in Democratic of Congo.

Table 4.10 :

Mobile Banking Security Framework

Mobile Banking Security Framework	M	SD
The security framework in our bank has enhanced Mitigation plans on security risk to mobile banking, assets, data, and capabilities	2.61	1.08
Our bank has developed and implemented the appropriate safeguards protect critical infrastructure mobile banking eservices in its security framework.	3.03	1.11
Our bank has in place appropriate Protection strategies of mobile banking events through the security framework.	2.74	1.21
The existing security framework in our bank carries with it Risk measures for mobile banking activities to take action regarding a detected insecurity event.	2.47	1.35
Confidentiality of customers' mobile banking is always ensured in our bank	2.63	1.17
The existing security framework ensures Integrity of customers mobile banking information	3.36	1.28
Our bank ensures that the customer mobile banking data is always available to the stakeholders on demand	2.84	1.20
Average Mobile Banking Security Framework	**2.81**	**1.20**

Source: Research data (2019)

The respondents were neutral on average mobile banking security framework (M=2.81, SD=1.20). They disagreed that the current safety system in their banks incorporated risk mitigation to fix a detected vulnerability event for M-banking. (M = 2.47, SD = 1.35) and exhibited neutrality on the following indicators that; confidentiality of customers' mobile banking was always ensured in their bank (M=2.62, SD=1.17), the security framework in their banks has enhanced mitigation plans on security risk to mobile banking, assets, data, and capabilities (M=2.61, SD=1.08); their banks had developed and implemented the appropriate safeguards protect critical infrastructure mobile banking eservices in their security framework (M=3.03, SD=1.11); their banks have in place appropriate protection strategies of mobile banking events through the security framework (M=2.67, SD=1.23) and that their banks ensure that the customer mobile banking data is always available to the stakeholders on demand (M=2.84, SD=1.20). They displayed neutrality on the claim that the existing security framework ensures Integrity of customers mobile banking information (M=3.36, SD=1.28).

Out of the result existing security framework in their banks carried low risk measures for mobile banking activities to take action on in case of a security event. The confidentiality of customer's mobile banking was not ensured. The security framework in their banks was moderately enhancing mitigation plans on security risk to mobile banking, assets, data and capabilities. The banks had developed and implemented appropriate safeguards in their security framework as well as having appropriate protection strategies. The banks also ensured that customer mobile banking data was always available to stakeholders on demand. The existing security framework highly ensured integrity of customers' mobile banking information.

4.5 Framework Validation

The research tried to determine whether the IVs were DVs' predictors by checking for the presence of meaningful association between both the IVs and the DV. Consequently, the thesis performed a correlation analysis and multiple regressions of all the variables. Thus, the research analysis was seeking to determine whether; sensitive organizational details, weaknesses in networks, threats to critical assets in information systems, and risks on CIS were estimators of M-banking protection mechanism among retails banks in DRC information systems critical assets, and risks on CIS.

4.5.1 Diagnostics testing

Before seeking estimating the model it was important to assure that accurate data is used and accordingly, appropriate diagnostic tests on; normality, multicollinearity, heteroscedasticity, and autocorrelation were conducted.

Normality Tests

This test produces probability value (p-value) which is used to signify normality or no-normal data (Onyango & Olando, 2020). Time when P-Value exceeds 0.05 is an implication of normally distributed data where the residual are asymptotically normal otherwise the data is not normally distributed. Abnormal data requires to be normalised that it can be used in regression. In that the sample population surpassed 50, Kolmogorov-Smirnov was used for normality test for yielding Table 4.11 results.

Table 4.11:

Results Tests for Normality

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Mobile banking security framework among commercial banks in Democratic of Congo	0.193	187	0.000	0.912	187	0.000
Critical organisational information	0.282	187	0.000	0.866	187	0.000
Threats to information systems critical assets	0.145	187	0.000	0.927	187	0.000
Infrastructure Vulnerabilities	0.300	187	0.000	0.819	187	0.000
Risks	0.170	187	0.000	0.895	187	0.000

a. Lilliefors Significance Correction

Source: Research data (2019)

Such results display abnormally distributed data each variable had a p-value beneath 0.05. The p-value for; Mobile banking security framework among commercial banks in Democratic of Congo was 0.000; critical organisational information was 0.000, threats to information systems critical assets was 0.000, infrastructure vulnerabilities was 0.000, and risks on CIS was 0.000. Accordingly, the data was non-normal and was therefore normalized to producing Table 4.12 results.

Table 4.12:

Normality results of Normalised data

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	Df	Sig.
Mobile banking security framework among commercial banks in Democratic of Congo	0.056	187	0.200*	0.988	187	0.123
Critical organisational information	0.064	187	0.059	0.986	187	0.052
Threats to information systems critical assets	0.063	187	0.069	0.975	187	0.002
Infrastructure Vulnerabilities	0.064	187	0.063	0.987	187	0.086
Risks	0.063	187	0.067	0.977	187	0.004

**. This is a lower bound of the true significance.*

a. Lilliefors Significance Correction

Source: Research data (2019)

This time the results signal normally distributed variable in that the p-value of each surpassed 0.05; mobile banking security framework among commercial banks in Democratic of Congo was 0.200; critical organisational information was 0.059, threats to information systems critical assets was 0.069, infrastructure vulnerabilities was 0.063, and risks on CIS was 0.067.

Testing for Multicollinearity

The research checked the presence of multicollinearity among the independent variables to insure that no control variable were measuring similar relationship as another variable or combination of variables was measuring. Multicollinearity occurs where the Variance Inflation Factor (VIF) exceeds 10 and the tolerance is below 0.1. in this research, the Table 4.13 captured these results.

Table 4.13:

Results of Multicollinearity Test

Variable	**Collinearity Statistics**	
	Tolerance	**VIF**
Critical organisational information	0.877	1.141
Threats to information systems critical assets	0.989	1.012
Infrastructure Vulnerabilities	0.888	1.126
Risks	0.960	1.042

Source: Research data (2019)

After the tests, the VIF produced each IV was lower than 10; critical organisational information (VIF = 1.141; threats to information systems critical assets (VIF = 1.012); infrastructure vulnerabilities (VIF = 1.126); and risks on CIS (VIF = 1.044). The tolerance for each was greater that 0.1; critical organisational information (Tolerance = 0.877; threats to information systems critical assets (Tolerance = 0.989); infrastructure vulnerabilities (Tolerance = 0.888); and risks on CIS (Tolerance = 0.960). Thus, for each, the tolerance was greater than 0.1 or 10% am indication that no multi-collinearity in any of the IV. Thus; critical organisational information, infrastructure vulnerabilities, threats to information systems critical assets, and risks on CIS are reliable estimator of the suggested model.

Heteroscedasticity Problem Tests

Now this assumption indicates that the probability distribution of the error terms remains the same for all experiments. In other terms, the variance of each term of error is the same for all results of the IVs. Furthermore, if the factors of variation do not have the same variance, this state of non-homogeneity of variance is known as heteroscedasticity (Tsegaye, 218). The research tested for heteroscedasticity using the Glejser test as shown in Table 4.14. It is observed that there is heteroscedasticity between variables if the p-value is less than or equal to 0.05. This test shows that if the P-value is important at 95 % confidence interval, the data has a problem with heteroscedasticity, but if the p-value is small (greater than 0.05), the data will not have a problem with heteroscedasticity.

Table 4.14:

Heteroscedasticity Problem Tests

Coefficients[a]

	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	0.011	0.210		0.052	0.959
Critical organisational information	0.001	0.039	0.002	0.030	0.976
Threats to information systems critical assets	0.000	0.030	0.001	0.012	0.990
Infrastructure vulnerabilities	-0.003	0.046	-0.005	-0.068	0.946
Risks on CIS	-0.003	0.032	-0.006	-0.082	0.935

a. a. *Dependent Variable: Unstandardized Residual*

Source: Research data (2019)

Out of these results, the p-value of each IV surpasses 0.05; Critical organisational information (p-value = 0.976, Threats to information systems critical assets (p-value = 0.990), infrastructure vulnerabilities (p-value = 0.946), and risks on CIS (p-value = 0.935 a proof heteroscedasticity absence.

Autocorrelation Assumptions Tests

In fact, the analysis checked hypotheses for autocorrelation that suggest zero covariance of error conditions over time. This means that the errors associated with one measurement are not compatible with the errors of any other measurement (Creswell, 2014). The research used the best known method for the identification of serial similarity, the Durbin Watson method. Absence of autocorrelation problem means that the terms of error are not associated with each other for different findings in this analysis.

Table 4.15:

Autocorrelation Assumptions Tests

Durbin-Watson
1.843

a. Dependent Variable: Mobile banking security framework among commercial banks in Democratic of Congo

b. Predictors: (Constant), Risks, Threats to information systems critical assets, Infrastructure Vulnerabilities, Critical organisational information

Source: Research data (2019)

The findings indicate that the Durbin-Watson was 1.843, and ranged between 1.5 and 2.5, suggesting that there were no autocorrelation problems with the data objects.

4.5.2 Correlation analysis

The research first examined the presence of a statistically meaningful association between the IVs and the DV by performing a correlation review to achieve the findings indicated in Table 4.16.

Table 4.16:

Results on Correlation analysis of Study variables

Correlations

		Mobile banking security framework among CBs in DRC	Critical organisational information	Threats to IS critical assets	Infrastructure Vulnerabilities	Risks
Mobile banking security framework among CBs in DRC	Pearson Correlation	1				
	Sig. (2-tailed)					
	N	187				
Critical organisational information	Pearson Correlation	.268**	1			
	Sig. (2-tailed)	.000				
	N	187	187			
Threats to information systems critical assets	Pearson Correlation	.202**	-.034	1		
	Sig. (2-tailed)	.006	.645			
	N	187	187	187		
Infrastructure Vulnerabilities	Pearson Correlation	.217**	.321**	-.079	1	
	Sig. (2-tailed)	.003	.000	.280		
	N	187	187	187	187	
Risks	Pearson Correlation	.437**	.177*	.060	.114	1
	Sig. (2-tailed)	.000	.015	.416	.120	
	N	187	187	187	187	187

***. Correlation is significant at the 0.01 level (2-tailed).*

**. Correlation is significant at the 0.05 level (2-tailed).*

Source: Research data (2019)

There, the results showed that there was a strong association for each IV and DV, which was large as the coefficient of correlation (r) for each contrast for IV and DV was greater than 0.5.Risks protection security strategy and mitigation plan the highest relationship (r = 0.437), then identifying critical organisational information (r = 0. 268), followed by analysing infrastructure vulnerabilities (r = 0.217) then, and lastly identifying threats to information systems critical assets (r = 0. 202). Protection security strategy and mitigation plan exhibited a moderate relationship (r = 0.437; p-value = 0.000) and identifying critical organisational information had a low one (r = 0. 268; p-value = 0.000) as well analysing infrastructure vulnerabilities which also had a low relationship (r = 0.217; p-value = 0.003) as well as identifying threats to information systems critical assets which too had a low with M-Banking Security Framework for commercial banks in DRC (r = 0. 202; p-value = 0.006). Each significantly related to M-banking Security Framework for commercial banks in DRC since each of the p-value was less than 0.05. Each of the IV had a significant positive relationship with Mobile banking Security Framework for commercial banks in DRC.

4.5.3 Regression Analysis

In conducting multiple regression analysis, the research regressed; identifying critical organisational information, identifying threats to information systems critical assets, analysing infrastructure vulnerabilities, and protection security strategy and mitigation against the dependent variable (Security Framework for commercial banks in DRC) using the equation (1) in section 3.7.

Testing goodness of fit

The study carried out an Analysis of Variance (ANOVA) to estimate the model's goodness of fitness, and these results are captured in Table 4.17.

Table 4.17:

ANOVA for Security Framework for commercial banks in DRC

ANOVA[a]

	Sum of Squares	Df	Mean Square	F	Sig.
Regression	30.493	4	7.623	17.65	.000[b]
Residual	78.606	182	0.432		
Total	109.099	186			

a. Dependent Variable: Mobile banking security framework among commercial banks in Democratic of Congo

b. Predictors: (Constant), Risks, Threats to information systems critical assets, Infrastructure Vulnerabilities, Critical organisational information

Source: Research data (2019)

The research evaluated whether the model's passed it goodness of fit to quality it for adoption by assessing the coefficient of the predictors expressed by X1, X2, X3 and X4 (that is their beta values), so that if all the alpha values are zero "0" (referring to the suggestion that each of β1, β2, β3 and β4 is zero) then the model is disqualified from being fit for use. However, if one, a combination or all of the beta value is not "0" then such as model if good for justifying its use in determining the framework. This ANOVA, which was premised on the 5% level of significance, yielded the results showing p-value as being 0.000 and F-statistics as 17.65). In these results, a p-value of 0.000 does not reach 0.05 in which case the implies at one, a combination or all of the beta values was not equally to zero and therefore the model was accepted. So, the research determined that at 0.05 significance level, there is ample proof to believe that at least one of or a combination; recognizing critical organisational information, recognizing sensitive infrastructure information systems, infrastructure vulnerabilities analysis, and protection security strategy and mitigation plan was useful in estimating the M-banking Security Framework for DRC's retail banks and The research can therefore approximate a model illustrating the M-Banking Security framework for Commercial Banks (CBs) in the DRC under these variables. As a result, the regression model is important with the F coefficient of 17.65 and P<0.000, which means that the points are fairly similar to the line of best fit in the scatter diagram. This suggests that the model is reasonably sufficient to understand the variation in the level of the DRC Security System for Commercial Banks, as shown by the variation in these parameters.

In order to approximate the research model, the IVs and DV were then regressed and the outcome of the analysis can be seen in Table 4.18.

Table 4.18:

Regression Results of Dependent Variable against Predictor Variables

Coefficients[a]

	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	0.592	0.336		1.763	0.080
Identifying critical organisational information	0.151	0.062	0.163	2.428	0.016
Identifying threats to information systems critical assets	0.149	0.048	0.195	3.087	0.002
Analysing infrastructure vulnerabilities	0.152	0.074	0.137	2.047	0.042
Protection security strategy and mitigation plan	0.304	0.051	0.381	5.936	0.000

a. Dependent Variable: Mobile banking security framework among commercial banks in Democratic of Congo

Source: Research data (2019)

Hypothesis Testing

This research examined the results of defining vital organizational knowledge using the following assumptions;

H_0: Identifying critical organisational information has no significant influence on Security Framework for commercial banks in DRC.

H_1: Identifying critical organisational information has significant influence on

Using the results in Table 20 it can be seen that p-value is 0.016 with t-statistics was 2.428 leading rejection of H_0 and accepting H_1 at 5% significance level in that p-value was less than 0.05. Accordingly, at 0.05 level of significance, there is ample proof identifying critical organisational information is not zero and therefore identifying critical organisational information is useful as an estimator of security framework for M-banking among retail banks in DRC.

The research used the following hypothesis to test the effect of the detection of risks to sensitive critical information systems assets;

H_0: Identifying threats to information systems critical assets does not significantly influence the Security Framework for commercial banks in DRC.

H_1: Identifying threats to information systems critical assets significantly influences the Security Framework for commercial banks in DRC.

Referring to Table 20, it is seen that while p-value was 0.002 and t-statistics was 3.087, which clearly specifies that p-value was less than 0.05. Owing to this H_0 is rejected while

H_1 was accepted. So, it clear than at 0.05 level of significance, There is abundant proof that the recognition of threats to information systems critical assets is not zero and that the recognition of threats to information systems critical assets is important as an integrator of security Framework for retail banks in DRC.

The involvement of analysing infrastructure vulnerabilities signified by the hypotheses;

> *H_0: Analysing infrastructure vulnerabilities does not significantly influence Security Framework for commercial banks in DRC.*
>
> *H_1: Analysing infrastructure vulnerabilities significantly influences Security Framework for commercial banks in DRC.*

In reference to Table 20, while p-value had a value 0.042, t-statistics registered 2.047 showing the p-value as being less than 0.05.in that the p-value was significant, there was rejection of H_0 and accordingly, acceptance of *$H_{1.}$* Owing to this then the research determined there is ample proof to declare that analysing infrastructure vulnerabilities is not zero and therefore analysing infrastructure vulnerabilities is valuable for predicting security framework for M-banking among retail banks in DRC.

Finally, the impacts of the defense policy and mitigation program were checked using the assumption;

> *H_0: Protection security strategy and mitigation plan does not significantly influence Security Framework for commercial banks in DRC in Garissa County.*

H_1: Protection security strategy and mitigation plan significantly influences Security Framework for commercial banks in DRC in Garissa County.

While consulting Table 20, it is found that at 0.05 significance level, while p-value recorded 0.000, the t-statistics registered 5.936. On noting that the p-value of 0.000 was much less than 0.05, the research rejected the H_0 while accepting H_1. Thus, there is ample proof that at 0.05 level of significance, protection security strategy and mitigation plan is not zero and therefore it is valuable in predicting security framework for retails banks in DRC.

Out of the findings in Table 20, the detection of sensitive operational details, the identification of risks to strategic assets in information systems, the review of network weaknesses, and the vulnerability defense and mitigation approach were important assessments of the DRC M-banking security framework for Commercial Banks in that each predictor's p-value was below 0.05; an indication of significant relationship between each of these estimators and the DRC M-banking security framework for Commercial Banks. More specifically, these variables; recognizing sensitive operational details, identifying risks to strategic assets in information networks, assessing network weaknesses, and the security management policy and mitigation plan will predict the reaction., DRC M-banking security framework for Commercial Banks.

Notably, identifying threats to information systems critical assets and protection security strategy and mitigation plan, with p-values being 0.002 and 0.000 respectively, had strong and statistically significant influence on the nature of Security Framework for commercial banks in DRC even at 1%. Meanwhile identifying critical organisational information and analysing infrastructure vulnerabilities, whose p-value where 0.002 and 0.016 respectively had a statistically significant impact on the level of Security Framework for commercial banks in DRC at 5%.

Model Fitting

The coefficient for identifying critical organisational information (β_1= 0.151), identifying threats to information systems critical assets (β_2= 0.149), analysing infrastructure vulnerabilities (β_3=- 0.152), and protection security strategy and mitigation plan (β_4=-0.304) were contributed to the equation;

$Y = 0.592 + 0.151X_1 + 0.149X_2 + 0.152X_3 +0.304X_4$……………………. (iii)

Specifically implying that the Security Framework for commercial banks in DRC = 0.592 + 0.151 (identifying critical organisational information) + 0.149 (identifying threats to information systems critical assets) + 0.152 (analysing infrastructure vulnerabilities) + 0.304(protection security strategy and mitigation plan). It is therefore inferred that the constant levels of Security Framework for commercial banks in DRCs before incorporating the business innovation is 0.592. Through the examination of coefficients for identifying critical organisational information it had positive impact on M-banking Security Framework for commercial banks in DRC of 0.151 such that a change by one unit in identifying critical organisational information can result a 0.151 rate change on Security Framework for commercial banks in DRC in the same direction. Identifying threats to information systems critical assets also had positive impact on Security Framework for commercial banks in DRC of 0.149 to mean that a change by one unit in identifying threats to information systems critical assets can result a change on Security Framework for commercial banks in DRC by 0.149 units.

Also analysing infrastructure vulnerabilities had positive impact on Security Framework for commercial banks in DRC of 0.152 in which case a change by one unit in identifying threats to information systems critical assets yields a 0.152 rate of change on Security Framework for commercial banks in DRC. Protection security strategy and mitigation plan also had positive impact on Security Framework for commercial banks in DRC having 0.304 signifying that a change by one unit in identifying threats to information systems critical assets lead to a .0304 rate change on Security Framework for commercial banks.

More so, Coefficients of; recognition of sensitive operational information, detection of information system risks to essential assets evaluating network vulnerabilities, and defense management policy and mitigation plan are optimistic, suggesting a directly proportional relationship with the DRC Security M-banking framework for Commercial Banks.. Thus, an increase in any of; identifying critical organisational information, identifying threats to information systems critical assets, analysing infrastructure vulnerabilities, and protection security strategy and mitigation plan leads to an increase in Security Framework for commercial banks in DRC and vice versa. Thus an decrease in in any of these variables; identifying critical organisational information, identifying threats to information systems critical assets, analysing infrastructure vulnerabilities, and protection security strategy and mitigation plan leads to an increase in Security Framework for commercial banks in DRC.

4.5.3.5 Model Summary

The outcomes on the model are captured in the model summary seen in table 4.19.

Table 4.19:

M-banking Security Framework Model Summary

Model Summary

R	R Square	Adjusted R Square	Std. Error of the Estimate
.529[a]	0.2795	0.2637	.65719

a. Predictors: (Constant), protection security strategy and mitigation plan, identifying threats to information systems critical assets, analysing infrastructure vulnerabilities, identifying critical organisational information

Source: Research data (2019)

This model summary has it coefficient of determination a being 0.2795, an acknowledgement that 27.95 per cent of the variance in the Security framework for M-banking among retail Banks in the DRCs is clarified by improvements in; recognition of sensitive operational details; detection of risks to essential assets in information systems; examination of vulnerabilities in infrastructure; and defense of vulnerability and mitigation techniques. The main determinants of the Framework for M-banking among retail Banks in the DRC are therefore; recognition of sensitive operational details, identification of risks to critical assets in information systems, review of network vulnerabilities, and defense management policy and mitigation plan.

4.6 Discussions of findings

The report presented its discussions depending on the goals of the research; to; determine critical organizational information influencing the design of a mobile banking security framework for commercial banks in DRC, establish threats to information systems critical assets that prompting the design of mobile banking security framework for commercial banks in DRC, analyse infrastructure vulnerabilities prompting the design of mobile banking security framework for commercial banks in DRC, and analyse risks prompting the design of mobile banking security framework for commercial banks in DRC

4.6.1 Discussions on Critical organisational information

Such results in this segment are proof of Betelhem's (2017) study, which has developed a new system for the banking sector to ensure the security and exchanging of messages using the mobile banking button. The Betelhem study (2017) recommends further development of the customer-side URL inspection system for reliability and performance checking and further analysis of potential usability problems. As a result, the present research was conducted to establish a mechanism for usability issues with m-banking. That depends on what constitutes an appropriate standard of safety and a balance between usability and protection as demonstrated in the study by Padyab et al. (2014) that information and knowledge are also identified on the identification of genders because the genders are not bound by certain entities or processes. Padyab et al. (2014) further revealed that a company is able to identify information assets which are hidden deep within business processes and daily work routines. Thus, Commercial Banks in DRC can; identify information assets in a structured way, ensure business practice perspective incorporated into risk assessment process, enhance identification of information asset owners

According to the results of the Moyo report (2014), the study attempted to establish critical resources in commercial banks in the DRC by defining critical financial information assets, teacher information on personal data, custom application technology, database computers and telecommunications equipment used for networking. The study findings show that the critical information on mobile banking included; customers database, credits and withdrawals (depositing and withdrawing respectively), account opening (registration of the customers) for use of the m-banking facilities, information on balance inquiry, funds transfer information, alerts, information on bill payment, loans disbursed, airtime purchase, and loan application information in that order. These findings agree to the study by Audu (2018), who show that financial institutions are adapting to new technical advances through the launch of mobile services offering; balance analysis, transfer of money, billing, airtime purchasing, loan submission, account opening and credit and withdrawal warnings. As a result, banks in the DRC provide similar services in their m-banking.

However, this information subject to various threats which include; improper disposal, decommissioning, lack of awareness, user permission fatigue, no privacy protection best practice, phishing, spyware, spoofing attacks, diallerware,, congestion, vulnerabilities leading to malware installation, data leakage, unintentional data disclosure, surveillance, application malfunction, encryption weaknesses, weak app. distributor authentication mechanism' weak sandboxing, danger of mismanagement of the above risks is not properly handled by the organisation. Such research in Moyo (2014) showed that the key risks to these vital assets were allowed and unauthorized users of devices, ransomware, device failures, access paths and program incompatibilities.

In his study, Ashraf (2012) identified eight threats. Such threats can be classified as: people, computers, applications and records, and management. Depending on this classification and discussions with banking and IT security experts, the M-Banking Security Model was developed to be used to identify security controls and interventions, to carry out risk evaluations of M-banking in the context of devices and mobile apps, or to conduct field audits. Nonetheless, the intimidating methods used and the internet communication protocol used for the purpose of transmitting their payload are unique for Douramanis (2014). Ashraf (2012) has meanwhile discovered that specific threats occur when dealing with mobile banking safety aspects. Underlying these threats cannot properly address the privacy, credibility and availability of Mobile Safety Resources by safety monitoring and measures. Mobile security tools, the mobile app and private information therefore require protection.

The commercial banks in DRC essentially require to identify their critical organisational mobile banking data that concerns the customer. In this, respect they should ensure that there is proper protection of their key information technology for protecting their critical assets and security requirements. This should ensure that key areas of concern are not subjected to any threat and that threats to current security practices are always mitigated. The banks should create session for; proper disposal, commissioning, awareness, overcoming user permission fatigue, ensuring privacy protection best practice. Actions should be taken for mitigating instance of; phishing, spyware, spoofing attacks, diallerware,, congestion, vulnerabilities leading to malware installation, data leakage, unintentional data disclosure, surveillance, application malfunction, encryption weaknesses, weak app. distributor authentication mechanism' weak sandboxing. Importantly, there should be risk of mismanagement of the above threats.

Importantly, there should careful protection against data leakage and as well as the banks should initiate mechanisms for authenticating weak application distributor. As well as they should create an effective encryption of the customers information. Their spyware should always be up to date and any risk should be properly managed. The customer mobile banking information should tracked always in every transaction instance to avoid unintentional data disclosure. The passwords should be updated frequently and the user integrity level should have strong protection. There is need for an open-flow M-banking networks, encryption of all sensitive information, password authentication for all computers carrying essential m-banking information, and training of all users of personal security information systems. This is stated by Moyo (2014) who claims that vital CIS properties that need to be secured allow the responsible individual to adhere to information security in order to protect their CISs and that there should be technological checks to minimize security threats in their CISs. The use of the OCTAVE-small approach to risk management has been useful in building information security knowledge among CIS users.. These controls should instill on; customers database, credits and withdrawals, registration of the customers, balance inquiry, funds transfer information, alerts, information on bill payment, loans disbursed, airtime purchase, and loan application information. The core consideration in developing the framework are; properly addressing information technology systems, addressing attacks on banks critical assets, requiring sufficient oversight of compliance specifications for sensitive infrastructure and minimize risks to best activities.

4.6.2 Discussions on Threats to information systems critical assets

This research established that there was a moderate occurrence of threats including interruptions on customer mobile information with their banks having reported any loss or destruction of the information at some point. Current threats and vulnerabilities moderately affected customers' mobile data in some way. Banks had never experienced any disclosure or modification to the customer's mobile information. A study by Moyo (2014) found that risks posed by threats were caused by indispensability of properties in sensitive information infrastructure, breach in data privacy and secrecy. This leads to a lack of profitability and disruption to the image of the organization.

In regards to this, the threats lowly influenced information system critical assets. IT specialists did not have limited access to the data transmission network between the bank and the client is not as reliable as the weak encryption used. Operating for many updates has had a small impact on the vital properties of the information system. The vital assets management system was mildly affected by the current and unused administrative accounts in the MS Active Registry.; secure storage of confidential information; presence of appropriate disaster recovery and business continuity documentation; properly configured firewall; staff well aware of IS threats and secure storage of information. The Douramanis research (2014) showed that there are cyber-attacks that could threaten the SCADA network core. These attacks differ depending on the process they use, as well as the internet communication protocol (ICP) they use to transmit their payload.

So, commercial banks in DRC should identify their specific M-banking threats and then effectively enhance; high restrictions of IT specialists access on the system with data transfer between the banks, strengthen of encryption used, minimize as much as possible the operating patches, protect the used accounts in Directory; high security storage of confidential information. These banks should importantly implement appropriate disaster recovery and business continuity documentation; effective configuration of firewall. All the staff must be made aware of IS threats and secure storage of information through seminars, training and staff meeting. To minimize outstanding risks, research administrators and consumers pick, build and enforce specific security and mitigation approaches in accordance with their information structures and their level of competence.

Apparently, a robust data protection legal framework should be enacted for ensuring that banks transferring money using mobile banking operate within a legal framework when providing this service. The mobile banking legal framework needs to effective consider provisions to to money transfer protection, computer user credibility, integrity codes, electronic documentation, and device use monitoring.. The legal framework should also be reviewed to strengthen the Threats to information systems critical assetss to accommodate stringent measure on computer use.

The protection against vulnerabilities is characterized by restrictions of IT specialists access on the system with data transfer between the banks, strength of encryption used, level of operating patches, used and active administrative accounts in MS Active Directory; security storage of confidential information; presence of appropriate disaster recovery and business continuity documentation; configuration of firewall; staff awareness of IS threats and secure storage of information.

4.6.3 Discussions on Infrastructure vulnerabilities

The study established that key components were moderately protected against vulnerabilities while technical vulnerabilities were moderately mitigated. Current technologies partially affected customer mobile data, vulnerabilities for key customer mobile data components were moderately diverted and the banks provided average level of deterrence on customer mobile data. These results confirm the findings in the study by Rovito (2016) stating that the ability to identify non-obvious points of failure can be used by system engineers to express system awareness and have a holistic perspective of a complex network. There is a need to draw up a list of vulnerabilities and potential strategies, and to convey risk information to decision-makers and other stakeholders. In addition, the Taubenberger Report (2014) suggests an approach to resolving vulnerability detection errors using compliance specifications and business process models. Security specifications reflect the security needs of the company and decide that any vulnerability is a security risk to the business. Safety specifications for information assets are analyzed in the framework of the business process model in order to assess how security mechanisms are properly applied and managed.

Commercial banks should identify the risks facing mobile banking security and accordingly design relevant protection strategies, risk measures and mitigation plans. The security framework should protect the banks mobile banking information by detecting risk occurrence on customer mobile banking and countering such a risk in advance. There should be mitigation plans of risks to customer mobile banking information. These plans should include allowance for eliminating or protecting against prone of CIS assets to risks. Computers used for online banking should be protected passwords, integrity codes, and firewall. Meanwhile back-up device should be stored in strong room and company records should be kept in fire proof safes. Router and the network equipment should also be protected. The key components for consideration are for protection against these vulnerabilities, addressing technical vulnerabilities, mitigating current technologies, protecting against vulnerabilities on key customer mobile data components, and providing high level of deterrence on customer mobile data.

4.6.4 Discussions on Risks

The study established that risks have moderate influence in the design of mobile banking security framework. The banks information has low effect on detecting risk occurrence on customer mobile banking. However, mitigation of risks to organizational customer mobile banking information is moderate. It was found that CIS assets are lowly prone to risks. The study established that customer accounts, records program and customer reports were not prone to any risk. Computers especially those used for online banking were lowly influenced by the risks while back-up disks stored the strong room and company records were moderately influenced by the risks. On the other hand, router and the network equipment and company information were highly impacted by the risks. The results support Janulevicius' (2016) report, which concluded that automation of virtualization system risk analysis offers ample data to adapt and enforce security controls to ensure an optimal degree of protection.

The commercial banks in provide for protection against infrastructure vulnerabilities by identifying key components and positioning the appropriate defense against any vulnerabilities. The study suggests that the bank show review and as well design new protection strategies that address and mitigate; technical vulnerabilities, current technologies vulnerabilities, and vulnerabilities for key customer mobile data components. The banks should review the existing protection strategies for the purpose of increasing level of deterrence on customer mobile data. The evaluation of security criteria analyses structures, staff and physical parts of business operations and IT integrates and validates this methodology by contrasting a formal procedure with two best practices. Second, the precision of the risk analysis is compared to the best practice risk management methodology used by an insurance firm in a variety of real-world scenarios. Further, it is evaluated in an in-depth experiment using security professionals to assess risk more effectively through the use of business processes and safety requirements. So order to fix vulnerabilities, detect errors and include a safety criterion, Octave approaches that benefit from a clear evaluation of safety criteria in the market context during risk detection. The core consideration in risk mitigation are; detecting risk occurrence on customer mobile banking, mitigation of risks to organizational customer mobile banking information, customer accounts, records program, customer reports, protection of computers especially those used for online banking, back-up disks stored the strong room and company records. There is an important need to protect router and the network equipment and company information.

4.6.5 Mobile banking security framework

The study established that the existing security framework among commercial banks in DRC was performing poorly in term of risk measures for mobile banking activities security event. The confidentiality of customers’ mobile banking is not ensured. The security framework in their banks is moderately enhanced by the mitigation plans on security risk to mobile banking, assets, data and capabilities. The banks have developed and implemented appropriate safeguards in their security framework as well as having appropriate protection strategies. The banks also ensures that customer mobile banking data was always available to stakeholders on demand. However, the existing security framework highly ensures integrity of customers' mobile banking information. These results are consistent with Ochuko's (2012) E-banking Operational Risk Assessment report, which showed that the structure and evaluation tools offered strong predictions for risk analysis and inference in these frameworks. Thus, the findings obtained can be considered encouraging and valuable for both the introduction of the E-banking system and research scholars in this field. A research by Ashraf (2012) also showed that a variety of specific trends appeared when dealing with security aspects of mobile banking in the context of mobile apps and applications. If these concerns are not adequately handled by security controls and interventions, the underlying risks may threaten the secrecy, credibility and availability of mobile technology properties. Mobile security properties that require protection are mobile apps, smartphone software and private information.

However, the banks seek to ensure that customer mobile banking data is always available to stakeholders on demand and that integrity of customers' mobile banking information is ensured. low assurance of confidentiality of customers' mobile banking and the mitigation plans on security risk to mobile banking, assets, data and capabilities are weak despite the banks having developed and implemented appropriate safeguards in their security framework as well as having appropriate protection strategies.

CHAPTER FIVE

SUMMARY, CONCLUSIONS, AND RECOMMENDATIONS

5.1 Introduction

In this chapter is provided a summary of the results of the study, observations and suggestions taken on the basis of the findings. It also highlights more studies that require research holes. Overview, findings and recommendations were focused on the objectives of the study: to identify sensitive operational details that would affect the creation of a mobile banking security framework for commercial banks in the DRC; to identify risks to strategic assets in the information systems that would contribute to the implementation of a mobile banking security framework for commercial banks in the DRC, analyse infrastructure vulnerabilities prompting the design of mobile banking security framework for commercial banks in DRC, and analyse risks prompting the design of mobile banking security framework for commercial banks in DRC.

5.2 Summary

The study provide summary of findings which were categorised depending in the study objectives ascertain vital operational knowledge that affects the design of the M-Banking Security Framework for Commercial Banks in the DRC, define risks to sensitive information systems that facilitate the design of the M-Banking Security Framework for Commercial Banks in the DRC, evaluate the deficiencies in the network that contribute to the design of the M-Banking Security Framework for Commercial Banking.

5.2.1 Mobile banking security framework among commercial banks

The study found that the existing security framework among commercial banks is DRC rate lowly in risk measures for mobile banking activities to take action on in case of a security event. The confidentiality of customers' mobile banking is not ensured. The security framework in their banks is moderately enhanced by the mitigation plans on security risk to mobile banking, assets, data and capabilities. The banks have developed and implemented appropriate safeguards in their security framework as well as having appropriate protection strategies. The banks also ensures that customer mobile banking data was always available to stakeholders on demand. However, the existing security framework highly ensures integrity of customers' mobile banking information.

5.2.2 Summary of findings on critical organisational information

Overall, the study established that the critical information on mobile banking included; customers database, credits and withdrawals (depositing and withdrawing respectively), account opening (registration of the customers) for getting into m-banking services, information on balance inquiry, funds transfer information, alerts, information on bill payment, loans disbursed, airtime purchase, and loan application information in that order. The threats to this information was found to include; improper disposal, decommissioning, lack of awareness, user permission fatigue, no privacy protection best practice, phishing, spyware, spoofing attacks, diallerware, congestion, vulnerabilities leading to malware installation, data leakage, unintentional data disclosure, surveillance, application malfunction, encryption weaknesses, weak app. distributor authentication mechanism' weak sandboxing, danger of mismanagement of the above risks is not properly handled by the organisation.

The study established that the main threats to be addressed include; data leakage and weak application distributor authentication mechanism had a low impact. Improper disposal, surveillance, encryption weaknesses, application malfunction, weak sandboxing, spyware and risk of mismanagement of the threats if not adequately addressed by the organization moderately impacted mobile banking systems. Other threats are; unintentional data disclosure, user permission fatigue, vulnerabilities leading to malware installation, lack of awareness, no privacy protection best practice, diallerware, decommissioning, congestion and spoofing attacks highly impacted mobile banking systems, and phishing

This analysis revealed that critical organizational information has a moderate impact on the establishment of a mobile banking security platform among commercial banks in the DRC, as demonstrated by addressing information technology systems properly, addressing attacks on banks with critical assets, ensuring proper compliance with security criteria for critical assets, and alleviating security threats.

5.2.3 Summary of findings on critical assets information systems threats

The study showed that risks to the M-banking network have a small impact on vital assets of the information sector. If IT specialists may not have restricted access to the data transmission network between banks, the business is not as secure as the poor encryption used. Operating updates has a small impact on the vital properties of the information network. The vital assets management system is mildly affected by the current and unused administrative accounts in the MS Active Directory; secure storage of confidential information; presence of appropriate disaster recovery and business continuity documentation; properly configured firewall; staff well aware of IS threats and secure storage of information..

5.2.4 Summary of findings on infrastructure vulnerabilities

This analysis revealed that the flaws in infrastructure moderately trigger the creation of the mobile banking protection system. The key components are moderately protected against vulnerabilities while technical vulnerabilities were moderately mitigated. Current technologies partially affected customer mobile data, vulnerabilities for key customer mobile data components were moderately diverted and the banks provided average level of deterrence on customer mobile data.

5.2.5 Summary of findings on influence of risks

The study established that risks have moderate influence in the design of mobile banking security framework. The banks information has low effect on detecting risk occurrence on customer mobile banking. However, mitigation of risks to organizational customer mobile banking information is moderate. It was found that CIS assets are lowly prone to risks. Customer accounts, records program and customer reports are not prone to any risk. Computers especially those used for online banking are lowly influenced by the risks while back-up disks stored the strong room and company records were moderately influenced by the risks. Router and the network equipment and company information is highly affected by the risks.

5.2.6 Summary of Inferential Analysis

The study found that; identifying critical organisational information has positive significant influence on Security Framework for commercial banks in DRC, identifying threats to information systems critical assets has positive significant influence on the Security Framework for commercial banks in DRC., analysing infrastructure vulnerabilities has a positive significant influence Security Framework for commercial banks in DRC., and protection security strategy and mitigation plan has a positive significant influence Security Framework for commercial banks in DRC.

The study established that 5% level of significance, 27.95% of variation in security framework for retail banks in DRC is triggered by change in; identifying critical organisational information, identifying threats to information systems critical assets, analysing infrastructure vulnerabilities, and analysing risks and developing protection security strategy and mitigation plan. At 0.05 level of significance; security framework for commercial banks in DRC = 0.592 + 0.151 (identifying critical organisational information) + 0.149 (identifying threats to information systems critical assets) + 0.152 (analysing infrastructure vulnerabilities) + 0.304(protection security strategy and mitigation plan)

5.3 Conclusions

The study established that the existing security framework among commercial banks is DRC does not sufficiently address the risk measures for mobile banking activities to take action on in case of an insecurity event. There is

In conclusion, critical organisational information has a statistically significant and positive influence on the development of mobile banking security framework among commercial banks in DRC.

As a conclusion, the threats to critical M-banking assets statistically significantly and positively influences design of mobile banking security framework for commercial banks in DRC.

The study concludes that there is statistically significant and positive influence of infrastructure vulnerabilities moderately on the design of the mobile banking security framework.

In conclusion that risk mitigation has a statistically significant and positive influence in the design of mobile banking security framework.

The research reveals that sensitive operational knowledge, detecting threats to critical assets in information systems, evaluating vulnerabilities in networks, and assessing hazards, and designing defense management policy and mitigation plan are strong determinants of the DRC Commercial Bank Security Environment at 0.05 level of significance. In addition, 27.95 percent of variance in the DRC security environment is clarified by shift in: recognition of sensitive operational information, detection of risks to vital assets in information systems, review of weaknesses in networks, and risk analysis, and implementation of defense policy and mitigation plan.

5.4 Recommendations

5.4.1 Policy recommendations

The research suggests a proportionate regulatory mechanism to ensure that DRC commercial banks sustain active risk control within their mobile banking network. Consequently, the report suggests creating a robust risk system for banks selling M-Banking services. It also suggests that mFSPs establish a robust, proportionate structure under which there will be continuous, constructive regulation of mFSPs. This will ensure sufficient attention in detecting, tracking and managing the risks of the mobile channel while providing adequate space for risk-related technologies that could be omitted if existing, inflexible quality standards exist.

OCTAVE-s can be used with the assistance of producers' users' information (PUI) or their representatives during the mapping of data properties. PUI organisations participate in a collective discussion to discuss areas where data is conveyed through supporting resources. In addition, the identified information assets for further risk assessment are incorporated into OCTAVE. The results show that GBM's tools and guidance could classify communication channels with potential leaks. Accordingly, this study suggests that GBM may encourage the listing of data resources through interaction or genre platforms.

Accordingly, the suggests implementation of an octave-s based with five processes;

Process one will include defining sensitive organizational information in order to set up a special group for M-Banking offering banks to recognize essential M-Banking information resources and to develop a collection of impact requirements and current security practices for banks. The information obtained is significant for the creation of resource-based risk profiles.

The second process is to identify the threats to critical information system infrastructure by evaluating the aspects of the network in which customers of the data system provide their opinions on what is important and what is being done to secure those assets by the network. The development team will then define the critical asset's protection criteria, and then create a risk assessment for each asset. The risk profile should be established on; the details previously gathered from the different CIS users should be grouped; the critical assets listed, and the hazard profile for each critical asset should be established. The committee will also determine how the effects of established risks arise from; leakage or representation of sensitive information; deletion of useful or critical data; loss or deterioration of essential information; disruption of access to relevant information, equipment, software or services.

Process three involves finding vulnerabilities in infrastructure Key components of vulnerabilities are being checked (technological vulnerabilities) that could contribute to unauthorized action on sensitive property. This is a high-level survey to refine the threat profiles of infrastructure and technology practices. Physical reviews of computer hardware and components would be conducted to identify vulnerabilities that could be abused by threats.

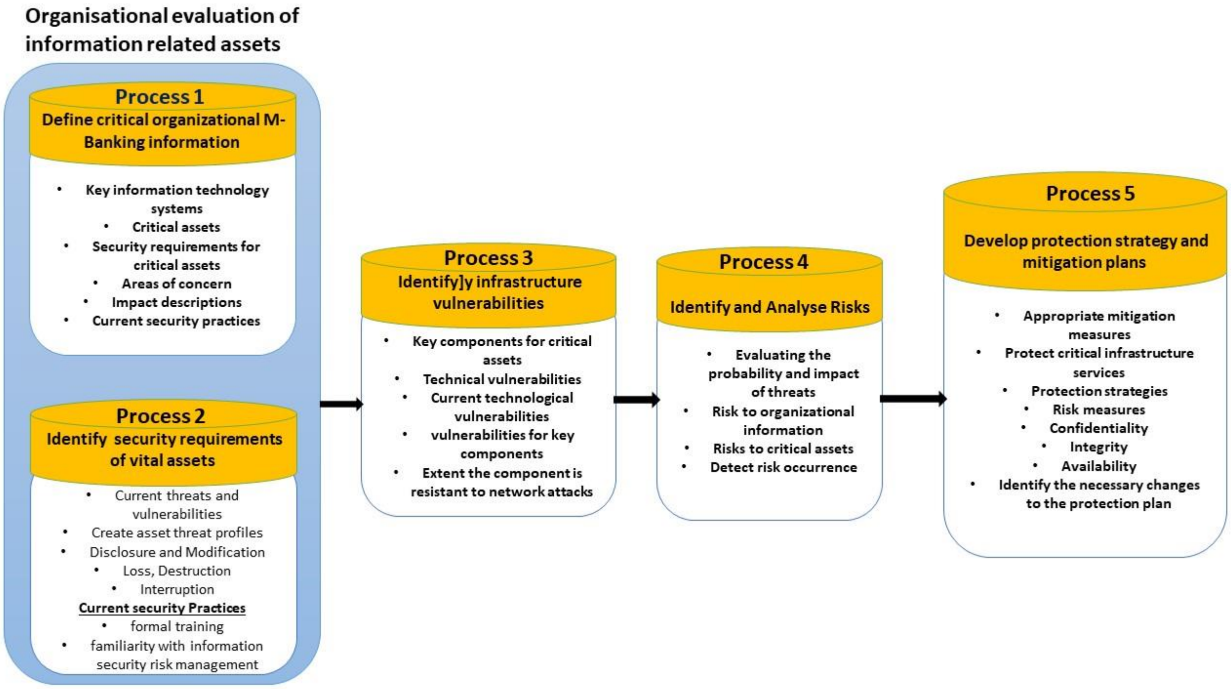
Process four and five includes a risk analysis and implementation of security management measures and mitigation plans. The group must define, assess and then take decisions on all risks to the core resources of the company. The team will now establish an organizational protection and prevention plan to tackle the vulnerability to essential infrastructure based on evidence obtained from analysis. The impact and probability of all identified risks will be qualitatively assessed in the risk analysis.

Framework Model

The proposed framework model captured in figure 10 should lead to the development of an organizational security policy and risk mitigation plan based on findings from process one to four.

Figure 5.1*:*

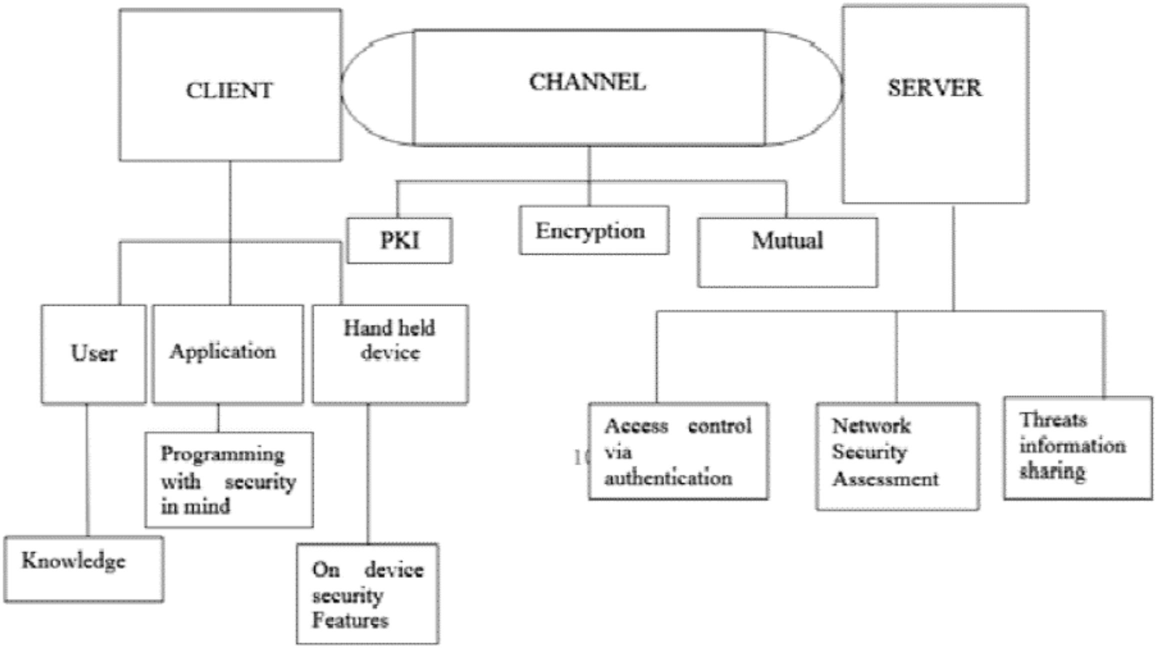
Proposed framework model


Organisational evaluation of information related assets
Process 1
Define critical organizational M-Banking information
• Key information technology systems
• Critical assets
• Security requirements for critical assets
• Areas of concern
• Impact descriptions
• Current security practices
Process 2
Identify security requirements of vital assets
• Current threats and vulnerabilities
• Create asset threat profiles
• Disclosure and Modification
• Loss, Destruction
• Interruption
Current security Practices
• formal training
• familiarity with information security risk management
Process 3
Identify]y infrastructure vulnerabilities
• Key components for critical assets
• Technical vulnerabilities
• Current technological vulnerabilities
• vulnerabilities for key components
• Extent the component is resistant to network attacks
Process 4
Identify and Analyse Risks
• Evaluating the probability and impact of threats
• Risk to organizational information
• Risks to critical assets
• Detect risk occurrence
Process 5
Develop protection strategy and mitigation plans
• Appropriate mitigation measures
• Protect critical infrastructure services
• Protection strategies
• Risk measures
• Confidentiality
• Integrity
• Availability
• Identify the necessary changes to the protection plan

The findings of the assessment using the framework model should lead to the development of an organizational security policy and risk mitigation plan based on safety practices. It should provide defense mechanism for protecting mobile banking, which is divided into three essential security layers, namely: The client; the communication channel and the server as capture hereunder.

Figure 5.2:

Security policy recommendation


CLIENT
CHANNEL
SERVER
PKI
Encryption
Mutual
User
Application
Hand held device
Programming with security in mind
Knowledge
On device security Features
Access control via authentication
Network Security Assessment
Threats information sharing

5.4.2 Recommendations on Research Findings

The made recommendations based on study findings as well as for future research, which are contained in this section. The study found that 27.95% of change in Mobile banking security framework among commercial banks in DRC is explained by; identifying critical organisational information has positive significant, identifying threats to information systems critical, analysing infrastructure vulnerabilities, and protection security strategy and mitigation. This means there are other factors accounting for the remaining 71.05%. The study therefore, recommends that other studies should be conducted to establish what contributes to the 71.05% variation in Mobile banking security framework among commercial banks in DRC.

REFERENCES

Akinleye, G. T & Kolawole, A. D. (2019). Internal Controls and Performance of Selected Tertiary Institutions in Ekiti State: A Committee of Sponsoring Organisations (COSO) Framework Approach. *International Journal of Financial Research*, 11(1), 405-416. https://www.researchgate.net/publication/337678534_Internal_Controls_and_Performance_of_Selected_Tertiary_Institutions_in_Ekiti_State_A_Committee_of_Sponsoring_Organisations_COSO_Framework_Approach.

Alberts, C. J. & Dorofee, A. (2001). *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVESM) Criteria (CMU/SEI-01-TR-016).* Carnegie Mellon University. http://www.sei.cmu.edu/publications/documents/01.reports/01tr016/01tr016abstract.html.

Alberts, C. J. & Dorofee, A. (2002). *Managing information security risks: The OCTAVE SM approach.* Addison-Wesley Anderson. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.461.7807&rep=rep1&type=pdf.

Alberts, C. J. & Dorofee, A. (2004). *Using Vulnerability Assessment Tools to Develop an OCTAVE Risk Profile.* Carnegie Mellon University. http://www.fish.com/satan/admin-guide-to-cracking.html.

Alberts, C., Dorofee, A., Stevens, J. & Woody, C. (2003*). Introduction to the OCTAVE Approach.* Carnegie Mellon University. https://www.itgovernance.co.uk/files/Octave.pdf.

Ashraf, I. (2012), *Mobile Banking Security. A security model* [Unpublished Doctoral Thesis]. Vrije Universiteit. http://www.vurore.nl/images/vurore/downloads/1073-Ashraf.pdf.

Audu, J. (2018). *Technology adoption in Democratic Republic of Congo (DRC): An Empirical study investigating factors that influence online shopping adoption* [Unpublished Master's Thesis]. University of Ottawa. https://ruor.uottawa.ca/bitstream/10393/37349/1/Audu_Janet_2018_thesis.pdf.

Bamrara, A. (2015) Evaluating Database Security and Cyber Attacks: A Relational Approach. *Journal of Internet Banking and Commerce (JIBC)*, 20(2), 1-17. https://pdfs.semanticscholar.org/0895/23b6af634dbfb6e194b4c9ba792b6523e7ee.pdf

Bankable Frontier Associates. (2008). *Managing the risk of mobile banking technologies*. Bankable Frontier Associates LLC. https://www.ifc.org/wps/wcm/connect/d39fa663-96dd-4d91-8036-e9893b1ced89/7.2+Managing+Mobile+Money+Risk.pdf?MOD=AJPERES&CVID=kbZlhJu.

Betelhem, B. G-H. (2017). *Conceptual security framework for mobile banking key authentication and message exchange protocols: Case of Ethiopian Banks* [Unpublished Master Thesis]. St. Mary's University. http://www.repository.smuc.edu.et/bitstream/123456789/3138/1/Security%20Framework%20for%20mobile%20banking.pdf.

Chin, R. W. K. (2012). *A Security Control Framework for Consumerization of Mobile Devices in the Bank Sector*. [Unpublished Masters Thesis]. Vrije University Amsterdam. https://silo.tips/queue/a-security-control-framework-for-consumerization-of-mobile-devices-in-the-bank-s?&queue_id=-1&v=1604125710&u=MTA1LjE2MC40MS45Ng==.

Creswell, J. W. (2014). *Research Design: qualitative, quantitative and mixed method approaches* (4th Ed.). SAGE Publications, Inc.

Desisa, A. & Beshah, T. (2014). Internet Banking Security Framework: The case of Ethiopian Banking Industry. *HiLCoE Journal of Computer Science and Technology*, 2(2), 1-7. https://www.hilcoe.net/wp-content/uploads/2020/08/V2N2Paper2.pdf.

Douramanis, M. (2014). *Risk assessment for the cyber threats to networked critical infrastructure* [Unpublished Master's Thesis] Leiden University. https://theses.liacs.nl/pdf/Douramanis-Michalis-non-confidential.pdf.

Esmaili, E., Desa M. I., Moradi, H. & Hemmati, A. (2011). The Role of Trust and Other Behavioral Intention Determinants on Intention toward Using Internet Banking. *International Journal of Innovation, Management and Technology*, 2(1), 95-100. http://www.ijimt.org/papers/111-E00102.pdf.

Ganthan, N. S., Rabiah, A. & Zuraini I. (2009). Adopting and Adapting Medical Approach in Risk Management Process for Analysing Information Security Risk?, *Risk Management for the Future – Theory and Casesi*, 34(5), 368–388, http://cdn.intechopen.com/pdfs/36111/InTech-adopting_and_adapting_medical_approach_in_risk_management_process_for_analysing_information_security_risk.pdf.

Gupta, S. K. & Rangi, R. (2014). *Research methodology. Methods, tools and techniques* (4th Ed.). Kalyan Publishers.

Hannula, T. (2018). *A framework for securing internal business-critical infrastructure services A structured approach for reducing systemic security gaps* [Unpublished Master's thesis] JAMK University of Applied Sciences is a university of applied sciences. https://www.theseus.fi/bitstream/handle/10024/156791/Hannula_Tero.pdf?sequence=1&isAllowed=y.

IT Governance Institute [ITGI]. (2007). *Framework Control Objectives Management Guidelines Maturity Models COBIT 4.1*. IT Governance Institute. https://www.bauer.uh.edu/parks/cobit_4.1.pdf

Janulevicius, J. (2016). *Method of information security risk analysis for virtualized systems* [Doctoral Dissertation]. Vilnius Gediminas Technical University]. http://dspace.vgtu.lt/bitstream/1/3026/1/J_Janulevicius_dissertation_LEIDYKLAI1.pdf.

Kothari, C. R. (2012). *Research methodology: Methods and techniques.* New Age International.

Kvale, S. (2007*). Doing interviews*. Sage.

Mazareanu, V. (2007). *Risk Management and Analysis: Risk Assessment Qualitative and Quantitative*. http://papers.ssrn.com/sol13/papers.cfm?abstractid=1549186.

Moyo, M. (2014). *Information security risk management in small-scale organisations: A case study of secondary schools? Computerised information systems* [Unpublished Master dissertation]. University of South Africa. DOI: 10.1109/ISSA.2013.6641062.

Mugenda, O. M. & Mugenda, A. G. (2008) *Research methods: Quantitative and qualitative approaches*. ACTS.

Ochuko, R. E. (2012). *E-banking operational risk assessment A Soft Computing Approach in the Context of the Nigerian Banking Industry* [Unpublished Doctoral Dissertation]. University of Bradford. https://bradscholars.brad.ac.uk/bitstream/handle/10454/5733/Rita%20Ochuko%20PhD%20Thesis.pdf?sequence=3&isAllowed=y.

Onyango, W. A. & Olando, C. O. (2020). Analysis on Influence of Bank Specific Factors on Non-Performing Loans among Commercial Banks in Kenya. *Advances in Economics and Business*, 8(3), 105-121. DOI: 10.13189/aeb.2020.080301

Padyab, A. M., Tero, P. & Harnesk, D (2014). Genre-Based Approach to Assessing Information and Knowledge Security Risks. *International Journal of Knowledge Management*, 10(2), 13-27 https://www.researchgate.net/publication/286183199_Genre-based_approach_to_assessing_information_and_knowledge_security_risks.

Pala, A. & Zhuang, J. (2019). Information Sharing in Cybersecurity: A Review. *Decision Analysis* 16(3),172-196. https://doi.org/10.1287/deca.2018.0387.

Panda, P. (2009). The OCTAVE-R approach to information security risk assessment. *Journal of Past Issues*, 4(3), 17-29, http://www.isaca.org.Journal/past-issues/2009/volume4/documents/jpdf09-OCTAVE.pdf.

Rhodes-Ousley, M. (2013). *Information Security*. (2nd Ed.). McGraw-Hill http://doi.org/10.15713/ins.mmj.3.

Rovito, S. M. (2016). *An Integrated Framework for the Vulnerability Assessment of Complex Supply Chain Systems* [Unpublished Master's Thesis]. Massachusetts institute of technology. https://dspace.mit.edu/bitstream/handle/1721.1/104816/959232903-MIT.pdf?sequence=1&isAllowed=y.

Shaaban, H. K. (2014). *Enhancing the governance of information security in developing countries: The case of Zanzibar* [Unpublished Doctoral Dissertation]. University of Bedfordshire. https://core.ac.uk/download/pdf/29821757.pdf.

Singh A. & Lilja, D. J. (2010). Criteria and Methodology for GRC Platform Selection. *Information System Audit and Control Association Journal*, 1(2010),1-1, https://www.isaca.org/resources/isaca-journal/past-issues/2010/criteria-and-methodology-for-grc-platform-selection

Storms, A. (2003). *Using vulnerability assessment tools to develop an OCTAVE risk profile.* http://www.sans.org/reading_room.

Taubenberger, S. (2014). *Vulnerability Identification Errors in Security Risk Assessments* [Doctoral Dissertation]. The Open University. http://oro.open.ac.uk/39626/1/Thesis%20-%20Taubenberger%20-%20Feb2014%20-%20Revised%20-%20Print.pdf.

Troy, G. (2012). *Mobile Banking Technology Options*. http://www.gsma.com/mobilefordevelopment/wpcontent/uploads/2012/06/finmark_mbt_aug_07.pdf.

Tsegaye, D. (2018). *Determinants of commercial banks' lending decision in Ethiopia: A case study on selected private banks* [Unpublished Masters Thesis]. Addis Ababa University. http://etd.aau.edu.et/bitstream/handle/123456789/12465/Dereje%20Tsegaye.pdf?sequence=1&isAllowed=y.

Uvaneswaran. S.M, Kassa, E. C. & Hamid, S. M. (2017). Challenges In E- Banking Services And Its Impact On Profitability Of Public Sector Bank In Ethiopia. *International Journal of Marketing & Financial Management*, 5(7), 36-46, DOI URL: http://doi.org/10.5281/zenodo.834863.

Uwadiae, O. (2013). COSO – *An Approach to Internal Control Framework. Financial Reporting*. Delloite. https://www2.deloitte.com/content/dam/Deloitte/ng/Documents/audit/Financial%20Reporting/ng-coso-an-appro ach-to-internal-control-framework.pdf.

APPENDIX I: RESPONDENTS' LETTERS

Introduction letter

Olivier Makeusa

Kenya Methodist University

P.O Box 45240, 00100

Nairobi

Contact +254718437442

makeusafumbu@gmail.com

Dear Respondent,

My name is Fumbu Makeusa a post graduate student at Kenya Methodist University conducting a research on Information Systems Security as a partial fulfillment for the award of degree of Master of Science in Computer Information Systems (MSc. CIS)

This questionnaire will take 15-20 minutes to fill and is meant to collect information that will be purely used for the research purpose. The information given will be treated with utmost confidentiality. This data will be critical in helping us come up with a risk based security model for the users of mobile banking.

I will appreciate your timely responses coming through before 1st Feb, 2019

Thanks in advance

Yours faithfully,

Olivier Makeusa

Admn. No. CIS-3-1739-1/2015

Kenya Methodist University

Nairobi

APPENDIX II: QUESTIONNAIRE

Demographic information

1. What is your gender? Please tick (√) in the correct Space

   Male [ ] Female [ ]

2. How long have you worked with the Bank? Please tick (√) in the correct Space

   1 to 5 years [ ] 6 to 10 years [ ] 11 to 15 Years
   [ ]

   16 to 20 Years [ ] Over 20 Years [ ]

3. What is your highest level of academic qualifications? Please tick (√)the correct Space

   Primary [ ] Secondary School Certificate [ ] College Diploma [ ]

   Undergraduate Degree [ ] Master's Degree [ ] PhD Degree [ ]

   Others [ ] Specify …………………………………………………..

4. How long have you been in the position? Please tick (√) in the correct Space

   1 to 5 years [ ] 6 to 10 years [ ] 11 to 15 Years
   [ ]

   16 to 20 Years [ ] Over 20 Years [ ]

5. How long have you been using banks information systems assets. Please tick (√) in the correct Space

   Not More than five years ( ) Between Six years and Ten years ( )

   Between 11 and 15 years ( ) Between 16 and 20 years ( )

   Between 21 and 25 years ( ) Between 26 and 30 years ( )

   Over 30 years ( )

6. How often do you receive formal training in using computer infromation systems. Please tick (√) in the correct Space

Not at All ( ) Once in a year ( ) Quarter yearly ( )

Monthly ( ) Weekly ( )

7. What is your level of familiarity with information security risk management. Please tick (√) in the correct Space

Not at All ( ) Low ( ) Moderate ( )

High ( ) Very high ( )

SECTION B: CRITICAL ORGANISATIONAL INFORMATION

8. Please tick **(√)** one appropriate box for each statement below to indicate whether you strongly agree (4), agree (3), Neutral (2), disagree (1) or strongly disagree (0) to the following statements on critical organisational information in your bank.

Scale: Strongly Disagree = 0: Disagree= 1: Neutral = 2: Agree = 3: Strongly Agree = 4

	Statement	**0**	**1**	**2**	**3**	**4**
(a)	Key information technology systems are properly protected in our bank					
(b).	The banks critical assets are have never been attacked by any threats					
(c)	Security requirements for critical assets are properly followed in our bank					
(d)	Areas of concern are not subjected to any threat					
(e).	Threats to impact descriptions have never affected the mobile banking					
(f)	Threats to current security practices are always mitigated					

9. Please in indicate in your own opinon the level of occurrence of the each of the following threats and vulnerabilities in your orginaisation's Computer Information System

	Not applicable	Low	Medium	High	Very high
Improper disposal					
Improper decommissioning					
Lack of awareness					
User permission fatigue					
Non privacy protection best practice					
Phishing					
Spyware					
Spoofing attacks					
Dialware					
Congestion					
Vulnerabilities leading to malware installation					
Data leakage					
Unintentional data disclosure					
Surveillance					
Application malfunction					
Encryption weaknesses					
Weak app distributor authentication mechanism					

Weak sandboxing					
Risk of mismanagement of the above threats if not adequately addressed by the organization					

SECTION C: THREATS TO INFORMATION SYSTEMS CRITICAL ASSETS

10. Please tick **(√)** one appropriate box for each statement below to indicate whether you strongly agree (4), agree (3), Neutral (2), disagree (1) or strongly disagree (0) to the following threats to information systems critical assets in your bank.

Scale: Strongly Disagree = 0: Disagree= 1: Neutral = 2: Agree = 3: Strongly Agree = 4

	Statement	**0**	**1**	**2**	**3**	**4**
(a)	Current threats and vulnerabilities do not affect the customers' mobile data in anyway					
(c)	Our bank has never experience any disclosure of customers mobile information					
(d)	There has never been any modification customers mobile information in our bank					
(e).	Our bank has never report any loss or destruction of customers mobile information					
(f)	There has never been any occurrence of interruption on customers mobile information					

11. Please tick **(√)** one appropriate box for each statement below to indicate whether you strongly agree (4), agree (3), Neutral (2), disagree (1) or strongly disagree (0) to the following threats to information systems critical assets in your bank.

Scale: Strongly Disagree = 0: Disagree= 1: Neutral = 2: Agree = 3: Strongly Agree = 4

	Statement	**0**	**1**	**2**	**3**	**4**
(a)	IT specialist have restricted access in the system.					
(b).	Data transfer between the bank and the company is very secure as only a weak encryption is used.					
(c)	The operating systems e.g. of the accounting system have several patches.					
(d)	The firewall is properly configured; websites are not blocked.					
(e).	All used and active administrative accounts in MS Active Directory.					
(f)	Staff are aware about IS threats.					
(g)	There is appropriate disaster recovery and business continuity documentation.					
(h)	Documents and information are securely stored					
(i)	Confidential information is securely stored					

SECTION D: INFRASTRUCTURE VULNERABILITIES

12. Please tick **(√)** one appropriate box for each statement below to indicate whether you strongly agree (4), agree (3), Neutral (2), disagree (1) or strongly disagree (0) to the following infrastructure vulnerabilities in your bank.

Scale: Strongly Disagree = 0: Disagree= 1: Neutral = 2: Agree = 3: Strongly Agree = 4

	Statement	**0**	**1**	**2**	**3**	**4**
(a)	Key components for critical assets are protected against vulnerabilities in our bank					
(b).	Technical vulnerabilities on customer mobile data are properly mitigated					
(c)	Current technological vulnerabilities do not affect customer mobile data					
(d)	vulnerabilities for key customer mobile data components are always diverted					
(e).	Our bank provides a very high level of deterrence and (or) defense provided on customer mobile data					

SECTION D. RISKS

13. Please tick **(√)** one appropriate box for each statement below to indicate whether you strongly agree (4), agree (3), Neutral (2), disagree (1) or strongly disagree (0) to the following risk on critical customer mobile banking assets in your bank.

Scale: Strongly Disagree = 0: Disagree= 1: Neutral = 2: Agree = 3: Strongly Agree = 4

	Statement	**0**	**1**	**2**	**3**	**4**
(a)	Risk to organizational customer mobile banking information is always mitigated					
(b).	There are no risks to critical customer mobile banking assets					
(c)	Our banks information always detect risk occurrence on customer mobile banking					

14. In your opinion, may you please indicate the level of influence of each of the following Computer Information System assets are prone to risk by ticking (√) the space corresponding to the correct answer?

Scale: Not at All = 1; Low = 2; Moderate = 3; High = 4; Very High = 5

	Statement	**1**	**2**	**3**	**4**	**5**
(a)	Computers especially those used for online banking.					
(b).	Records program					
(c)	Customers' accounts					
(d)	Customers reports					
(e).	Back-up disks stored the strong room					
(f)	Company records					
(g)	Company information					
(h)	Router and the network equipment					

SECTION E: MOBILE BANKING SECURITY FRAMEWORK AMONG COMMERCIAL BANKS IN DEMOCRATIC OF CONGO

15. Please indicate your level of agreement or disagreement with the following statements in regards to framework in your bank. Please tick (√) the space corresponding to the correct answer in each question below

Scale: Strongly Disagree = 0: Disagree= 1: Neutral = 2: Agree = 3: Strongly Agree = 4

Statement	**0**	**1**	**2**	**3**	**4**
The security framework in our bank has enhanced management of security risk to mobile banking, assets, data, and capabilities					
Our bank has developed and implemented the appropriate safeguards to ensure delivery of critical infrastructure services using its security framework.					
Our bank has developed and implemented the appropriate activities to identify the occurrence of an insecurity of mobile banking event through the security framework.					
The existing security framework in our bank enhances development and implementation of the appropriate mobile banking activities to take action regarding a detected insecurity event.					
The existing security framework ensures that our bank has develops and implements the appropriate activities to maintain mobile banking plans for resilience and to restore any capabilities or services that were impaired due to a insecurity event					

Thank you for your cooperation.

APPENDIX III: CHECK LISTS

SECTION A: IDENTIFY CRITICAL ASSETS IN MOBILE BANKING SYSTEMS

1. The main purpose of this section will be to identify and locate all information systems assets used to support administrative activities. Observation checklists and inspection checklists will be used to collect data from key users of mobile banking information systems.

Asset identification and inspection checklist

Important Asset	Type	Location

Critical assets

Critical asset	Justification for its selection

Organisational security practices

Item	**Policy**
Information security policy	
Risk management	
Access account management	
Configuration management	
Password authentication	
Network security policy	
Modems policy	
Cryptographic capability	
System administration	
Incident response capability	
Viruses and malware policy	
Contingency planning	
Backups policy	
Maintenance policy	
Media sanitization	
Physical security policy	
Personal security policy	
Training and awareness programmes	

Areas of concern for critical information systems assets

	Loss /destruction
	Interruption
	Modification
	Loss /destruction
	Interruption
	Modification
	Loss /destruction
	Interruption
	Modification
	Loss /destruction
	Interruption
	Modification
	Loss /destruction
	Interruption
	Modification
	Loss /destruction
	Interruption
	Modification
	Loss /destruction
	Interruption
	Modification
	Loss /destruction

	Interruption
	Modification
	Loss /destruction
	Interruption
	Modification
	Loss /destruction
	Interruption
	Modification

SECTION B: IDENTIFY THREATS TO CRITICAL MOBILE BANKING ASSETS

2. In this process research team will identify security requirements for critical assets and threats to those critical assets. Data will be gathered using customised OCTAVE-small worksheets. The study will identify the main threats to mobile banking as; Human actors using network access, Human actors using physical access, System problems such as hardware defects, software defects, unavailability of related enterprise systems, viruses, malicious code and other threats that are outside the control of an organisation such as; natural disasters, such as floods, earthquakes, storms and fire. Such threats could affect and mobile banking systems as well as interdependency risks such as the unavailability of critical infrastructures (telecommunications, electricity).

Identifying security requirements for critical assets

Key:
1 = Most important security requirement,
2 = Second most important security requirement
3 = Third important security requirement

Critical asset	Security requirements descriptions	Most important security requirement	Priority
		Integrity	
		Availability	
		Confidentiality	
		Integrity	
		Availability	

		Confidentiality	
		Integrity	
		Availability	
		Confidentiality	
		Integrity	
		Availability	
		Confidentiality	

3. Identifying threats to critical assets

Data will be collected using a customised OCTAVE-small threat profile worksheet, which will depcuit the common threats/threat sources in CISs critical assets, their effects and their overall impact on mobile banking systems.

Threats/threat sources from asset risk profiles

Asset affected	Threat/threat source	Possible threat effect or impact on asset	Potential impact on the banks' operations

Areas of concern pertaining to threats in critical assets

Index	Area of concern arising from	Affected information systems asset	Cited examples	Effects on critical information system asset
1				
2				
3				
4				
5				
6				
7				

SECTION C: IDENTIFY INFRASTRUCTURE VULNERABILITY

4. This section will be an examination of access paths involved identifying the key components of systems of interest which will be closely related to critical information systems assets

Systems of interest and key classes of components

RECORDS MANAGEMENT SYSTEM	
Key classes of components used to access this critical asset	
COMPUTERISED FINANCIAL RECORDS	
Key classes of components used to access this critical asset	
CUSTOMERS MASTER RECORDS	
Key classes of components used to access this critical asset	
Key classes of components used to access this critical asset	
Key classes of components used to access this critical asset	
Key classes of components used to access this critical asset	

Key classes of components and reasons for their selections

Class of Component	Reason for selection
Server-computer	Such as database storage
Networking components	Such as router / switched for providing connectivity and main access to LAN and internal/external access.
Security components	Such as firewall – key part of security for external access
Desktop workstations	Used for all internal access to server and other desktop computers. Financial records processing
Laptops	Used for internal and external access to the server computer
Storage devices	Provide storage media for the critical information
Wireless components	Providing connectivity and illegal access to records

Observation of physical security threats

Asset	**Location**	**Threats identified**

5. Simple system vulnerability checks will be performed on hardware and software. The vulnerability checks will be done while information systems assets were in use. An observation checklist will be used to collect data during the systems vulnerability checks

Observed vulnerabilities in the information systems

Target area	Observed Vulnerabilities	Comments

Frequently encountered hardware and software problems

Problem	Effects	Control in place

SECTION D: CONDUCT RISK ANALYSIS AND DEVELOP PROTECTION STRATEGIES AND MITIGATION PLANS

6. This section is intended to identify, analyse and evaluate risks to critical information systems assets. It will also be used to examine protection strategies and mitigation plans that banks could implement to safeguard the critical mobile banking information systems assets utilising the resources available in view of the identified risks

Proposed organisation protection strategy

Strategy Area	**Strategy**
Security awareness and training	
Information security strategy	
Information security risk management	
Security regulations	
Disaster recovery plan	
Physical security	
Information technology security	
Security staff	

Mitigation plans for critical assets

Threat Type	Actions
Financial accounting information risks mitigation plans	
Network infrastructure mitigation plans	

Risk Treatment

Threat source /vulnerability	Risk	Impact

OCTAVE-small- Risk Impact Evaluation Criteria

Impact Area	High	Medium	Low

APPENDIX IV: INTERVIEW GUIDE

My name is Fumbu Makeusa a post graduate student at Kenya Methodist University conducting a research on Information Systems Security as a partial fulfillment for the award of degree of Master of Science in Computer Information Systems (MSc. CIS). I thought it would be a good idea to interview you, so that I may gain sufficient information on security framework for mobile banking in the banking industry.

Purpose. I would like to ask you some questions about your background, your education, some experiences you have had, and some of your hobbies and interests in order to learn more about you and use this information in analysing data on security framework for mobile banking in the banking industry of Democratic of Congo.

Motivation. I hope to use this information to help banks in DRC are able offer more secured M-Banking services of customers, increase the number of customers using the M-Banking technologies and protects customers from hackers and third party access to their account information.

Time Line. The interview should take about 10 minutes. Are you available to respond to some questions at this time?

Transition: Let me begin by asking you some questions about yourself and your role in mobile banking and its security.

1. How long have you been using the information systems assets for mobile banking system?

2. Did you receive formal training in using computersied information systems on mobile banking system?

3. Are you familiar with information security risk management?

4. What information system assets does your banks have for mobile banking system?

5. What are the important information systems assets you need to protect?

6. Where are the identified information systems assets located?

7. May you please prioritized these information systems assets in terms of their importance, stating the rationale for selecting assigning their importance

8. May you please say the security issues you have encountered on customers mobile banking system since you started using the system in terms of:

    a. Hardware failures

    b. Software failure

    c. Loss of data integrity, confidentiality or availability through intentionally or unintentionally operations due to

        i. Your actions

        ii. Other authorised internal users

        iii. Unauthorised internal users

        iv. External users

        v. Malware

        vi. Hacking

        vii. Other factors

9. What was the severity of these security issues on the operations of mobile banking in your company?

10. May please you briefly explain how you responded to each of these problems?

11. What measures do you put in place to secure your customers' mobile data?

12. How do you check whether your customers' mobile banking data has been tempered with

13. What data recovery method do you use in the event that your computer has crashed?

14. What do you do if your computer is infected by a recently deployed virus?

15. What problems have you encountered with your mobile banking system?

16. How frequent has each of the problems been?

17. How effective was the initiative made in

    a. Solving the problem

    b. Preventing it from recurring?

18. How do you deal with those important files which do not open?

19. How secure is your mobile banking system from;

    a. internal intruders

    b. external intruders

c. unexpected hardware crashes

20. What mechanisms do you use to detect intrusions in your mobile banking system?

21. What methods of backups do you use and where do you store them?

22. How do you deal with virus problems?

23. What challenges do you face in securing your mobile banking system?

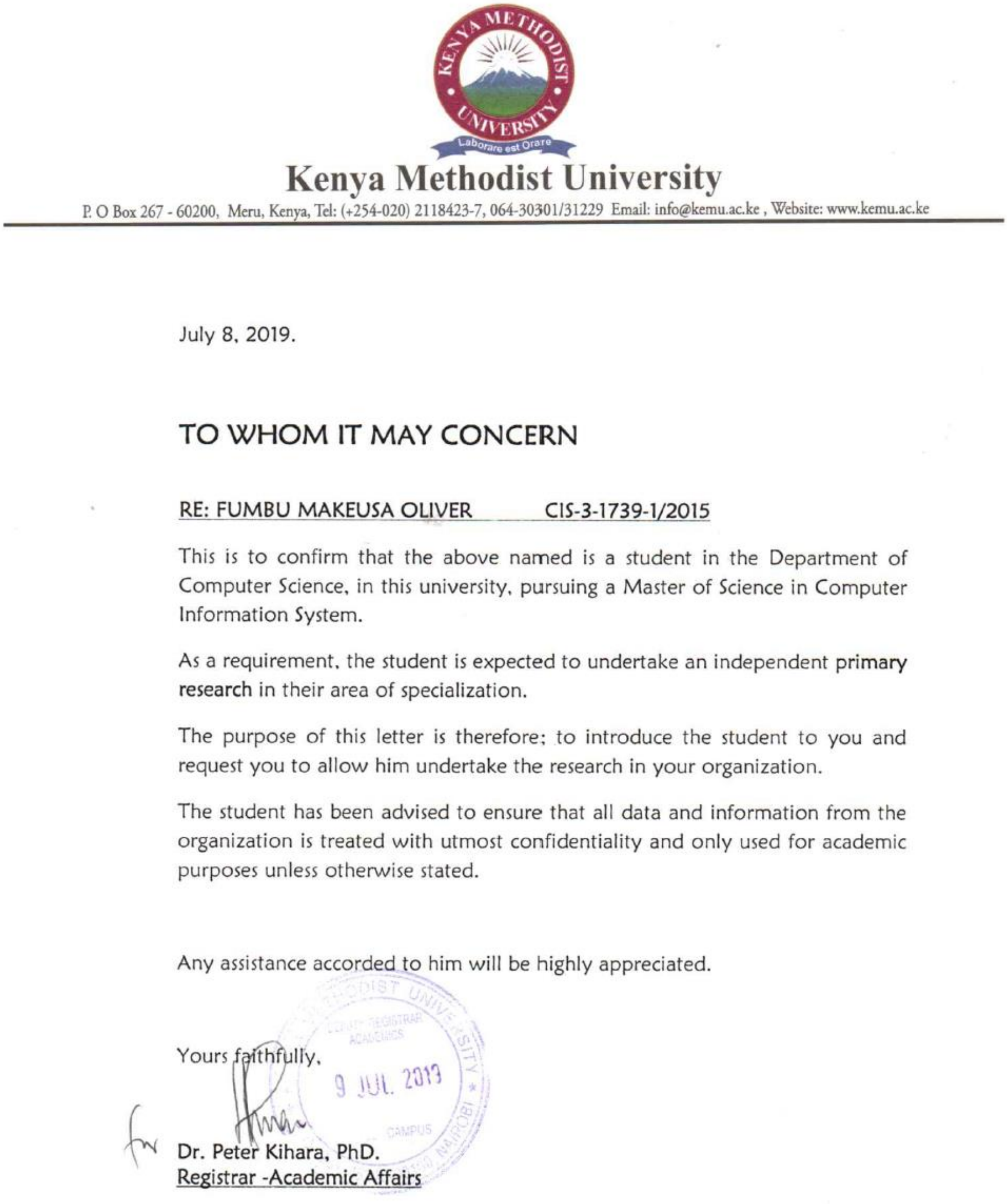
APPENDIX V: EXPECTED OUTPUTS

Expects outputs for each octave-small process

OUTPUT			
Identifying threats to mobile banking information systems critical assets	**Identifying threats to mobile banking information systems critical assets**	**Identify infrastructure vulnerabilities**	**Conduct risk analysis and develop protection security strategy and mitigation plan**
• Critical assets • Security requirements for critical assets • Areas of concern and impact descriptions • Current security practices	Current threats and vulnerabilities	• Key components for critical assets • Current technological vulnerabilities for key components	• Risk measures • Risks to critical assets • Protection strategies • Mitigation plans

Source: Panda (2009)

APPENDIX VI: DATA COLLECTION AUTHORISATION



Laborare est Orare

Kenya Methodist University

P. O Box 267 - 60200, Meru, Kenya, Tel: (+254-020) 2118423-7, 064-30301/31229 Email: info@kemu.ac.ke , Website: www.kemu.ac.ke

July 8, 2019.

TO WHOM IT MAY CONCERN

RE: FUMBU MAKEUSA OLIVER CIS-3-1739-1/2015

This is to confirm that the above named is a student in the Department of Computer Science, in this university, pursuing a Master of Science in Computer Information System.

As a requirement, the student is expected to undertake an independent **primary research** in their area of specialization.

The purpose of this letter is therefore; to introduce the student to you and request you to allow him undertake the research in your organization.

The student has been advised to ensure that all data and information from the organization is treated with utmost confidentiality and only used for academic purposes unless otherwise stated.

Any assistance accorded to him will be highly appreciated.

Yours faithfully,

METHODIST UNIVERSITY
DEPUTY REGISTRAR
ACADEMICS
9 JUL. 2019
CAMPUS
NAIROBI

for Dr. Peter Kihara, PhD.
Registrar -Academic Affairs