2022

A Framework for monitoring operational risks in claims processing: case of Sanlam Insurance Company.

Maraga, Emma Ikonge
Strathmore Business School
Strathmore University

A Framework for Monitoring Operational Risks in Claims Processing: Case of Sanlam Insurance Company

Emma Ikonge Maraga

(109962)

Master of Development Finance

2022

A Framework for Monitoring Operational Risks in Claims Processing: Case of Sanlam Insurance Company

Emma Ikonge Maraga

(109962)

A Thesis Submitted in Partial Fulfilment of the Requirements for the Degree of Master of Development Finance at Strathmore University

Strathmore Business School

Strathmore University

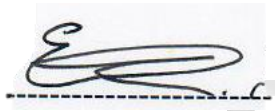
Nairobi, Kenya

October, 2022

DECLARATION

I declare that this work has not been previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, the dissertation contains no material previously published or written by another person except where due reference is made in the thesis itself. © No part of this thesis may be reproduced without the permission of the author and Strathmore University

Emma Ikonge Maraga



24th August, 2022

Approval

The dissertation of Emma I. Maraga was reviewed and approved by the following:

Dr. Vincent Omwenga (Supervisor)

Research Director, School of Computing and Engineering Sciences

Strathmore University

24th August, 2022

Dr. Angela Ndunge

Ag. Executive Dean

Strathmore University Business School.

Dr. Bernard Shibwabo

Director, Office of Graduate Studies

DEDICATION

This dissertation is dedicated first to GOD for the blessings of life and strength to complete this research and for HIS guidance. I would also like to thank my family who have been very supportive during this process, my two best friends who have pushed me and been patient with me, and lastly, my husband who has been a strong pillar of support and strength.

ACKNOWLEDGMENTS

I would like to thank my supervisor Dr. Omwenga for his continual support and help and time sacrificed in order to help me complete this project. He has been a source of knowledge and understanding with respect to the subject matter and has worked with me tirelessly in order to be able to finish this research. I would like to thank him profusely for taking me on as a research student. I would also like to thank the Strathmore Business School for their facilitation in order for me to complete this project.

ABSTRACT

Monitoring operational risks in the claim processing continue to present a challenge to many insurance firms. This is largely due to poor approaches used to monitor operational risk and many insurance firms have experienced capital losses, brand and reputation erosion. This study sought to propose a framework for monitoring operational risks in the claim processing using the decentralized Blockchain Technology taking a case study of Sanlam Insurance Company. To develop the proposed framework, the study was based on specific objectives that include: investigate the operational risks associated with the claims processing in the company; review the indicators of operational risks in claims processing in the company; review how information communication technology has been utilized to monitor operational risks by the company. The study adopted a qualitative research methodology with the primary data collection instrument being a semi-structured interview. Descriptive and inferential data analyses were conducted. From the study human error was the most prevalent operational risk (100%) followed by system failures (77%), accounting errors (55%) and fraud (44%). It was established that customer dissatisfaction (66.7%), IT failure (55.6%), and errors (44%) were the leading operational risk indicators. Further the study established the existence of a positive relationship between the operational risk indicators and the type of operational risks experienced by the insurance company. There was also a high level of adoption of ICT technology in the company (100%). The immutability characteristics of the Blockchain was considered more important by the respondents at an index score of 1.33 (33%). Based on the findings, the researcher proposes a framework that utilizes Blockchain Technology's immutability characteristics to monitor the claims processing in the company. The proposed framework would provide clients and insurance agents with the means of managing claims in a transparent, irrefutable and responsive manner.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

BT – Blockchain Technology

VaR – Value at Risk

OpVaR – Operational Value at Risk

IRA – Insurance Regulatory Authority

KRA – Kenya Revenue Authority

ERM – Enterprise Risk Management

USD – United States Dollar

AKI – Association of Kenyan Insurers

IIK – Insurance Institute of Kenya

GI – General Insurance

ORM – Operational Risk Management

IoT – Internet of Things

AI – Artificial Intelligence

UN – United Nations

P2P – Peer-to-Peer

GDP – Gross Domestic Product

WEF – World Economic Forum

EU – European Union

UK – United Kingdom

KRI – Key Risk Indicator

GARP – Global Association of Risk Professionals

NACOSTI – National Commission for Science, Technology and Innovation

RAG – Red, Amber, Green Indicator

CHAPTER ONE: INTRODUCTION

1.1. Background to the study

Operational risk in insurance worldwide has always been difficult to quantify, adequately measure, and monitor. This can be attributed to a culture of operational risk not being rooted in control processes, poor organisational structure, and work processes that don't allow an organisation to identify losses in data (Hermit and Arab, 2012). Similarly, operational risks are difficult to appropriately quantify due to their infrequency and uniqueness within companies (McShane, 2018). Lloyds of London and its franchises have identified that focus for operational risks should be on identification, management and monitoring. However, there is a need to acknowledge that operational risks can both be isolated or intertwined with other risk categories which further complicates its identification, measurement, management, and monitoring (Manning and Gurney, 2005). Furthermore, operational risks are organisational focused and therefore a general framework that can be used to manage risk that applies across a spectrum of company is difficult to come by. It is for this reason that this study narrows to a company specific so as to contextually analyse effectively the study constructs.

This study therefore focuses at proposing a framework for monitoring operational risks at Sanlam Insurance company with an aim of generalising it to cover the entire insurance sector since there are no public study findings on operational risk monitoring especially in one of the key processes within an insurer, claims processing. This chapter introduces operational risks, gives an overview of the Kenyan industry, discusses operational risks within the industry and technology used within the insurance industry, introduces Sanlam Insurance, and finally discusses the problem statement, objectives, and research questions.

1.1.1. Operational Risks in the Insurance Industry

Operational risks are considered to be the biggest cause of financial failures affecting many insurers worldwide (Hoffman, 2002). Traditionally, these risks have been difficult to quantify, insure and manage as they are found to be context driven and embedded in management culture, organisational structure, and the desires of those who manage risk (Power, 2006; Johnson, 2006). Operational risks therefore consist of failures resulting from

people, processes, systems, and/or external events. Despite these risks having been in existence for centuries; their impact on companies' profitability was often thought to be relatively insignificant. However, within the last few decades, recent trends in globalisation, global internet connectivity, improvements in technologies, and value chain dependencies, have made operational risks an increasingly significant source of risk (Chernobai, 2008).

In order to quantify operational risks, the insurance industry has relied on two key governance committees for Risk Management; the Basel Committee that has over the years set standards for defining and measuring operational risk; and solvency II which was introduced in the last decade in response to various insurers defaulting in the 2007/08 financial crisis. Solvency II was developed based on the three pillars of Basel II regulation (Wagner, 2014). Basel Committee is an internationally established committee that developed Basel I, II, and III standards that focus on banking supervision and has been widely adopted within the insurance industry for its defined categories for operational risk. It has three pillars namely: minimum capital requirements, supervisory review, and market discipline. Operational risk under the Basel Committee has evolved to an advanced measure of determining a firms' internal operational risk. Although Basel II/III has stronger focus within the banking industry with respect to maintaining high liquidity, it has been utilised widely within the insurance industry in the aid of categorising operational risks as there is no explicit Solvency II definition of operational risk quantification, and measurement (Gatzert, 2012). Solvency II mainly focuses on both financial and non-financial risks that are peculiar and non-systematic with lower correlation.

The insurance industry relies on two main frameworks; Basel II/III (especially relating to qualitative categorization of operational risks) and Solvency II (purely sets capital requirements for an insurer). Basel Committee on Banking Supervision (2004) breaks down operational risks into seven (7) categories: internal fraud; external fraud; Employment practices and workplace safety; clients, products and business practice; damage to physical assets; business disruption and systems failures; execution, delivery, and process management. These can be characterised by improper processing of policy documents due to inefficient systems, poor user understanding of systems, inaccurate claims procedures and controls leading to internal/external fraud, lack of compliance with provisions of insurance acts and other operational/legal risks, miscommunication of deadlines, inaccurate

processing of client data, vendor disputes, accounting or data entry inaccuracies, and other failures (Oscar ,, 2013). Solvency II establishes the need for insurers to hold capital reserves of 200% of the base capital for a fixed time horizon (up to one year) in order to act as a buffer in event of any unforeseen catastrophic events. Operational risks exist in every organisation due to influence and interaction of internal and external events, people, processes and technology; but their inappropriate management often leads to significant losses (Mitra ,, 2016).

Now more than ever, insurance and financial systems have become more complex and interconnected. This has led to challenges in understanding and mitigating operational risks which have become too tedious and complex. Over the past decade, at least nine (9) insurance companies in Kenya have collapsed as a result of poor operational risk management; attributed mostly to fraud (Insurance Regulatory Authority, 2017). This prompted IRA to establish a comprehensive risk management guideline for the insurance sector covering all risks, effective June 2013, with specific realisation of the correlation between the level of returns earned and operational risk.

Operational risks have been defined as the risks of adverse change in the value of capital resources of the company resulting from operational events such as inadequacy or failure of internal systems, personnel, procedures, or controls, as well as external events (International Association of Insurance Supervisors, 2020). Many of these risks arise as a consequence of conducting day-to-day business operations and are typically managed with little or no incident. It refers to the risk that results from inadequacies in the management of otherwise quantifiable risk and unforeseen external events that can impact an insurer. Some of the operational risks may include events and actions or inactions, such as fraud, human error, accounting errors and system failures.

Insurance companies including Sanlam Kenya can monitor and manage operational risks in claims processing. Policyholders can notify claim requests which are received by the insurer in order for them to begin claims processing. The claims processing procedure consists of notification which includes; all necessary documentation attached; policy checks and reviews used to check for validity; damage evaluation; and lastly, payment. At each given stage of the process, there can arise various operational risks. The likely operational risks of note include; Fraud (external or internal), inaccurate data entry, incorrect payment details, delays according to set timelines and reputational damage in the event of poor

customer service. Dealing with operational risk entails identification, analysis and mitigation, and monitoring of the different risk categories.

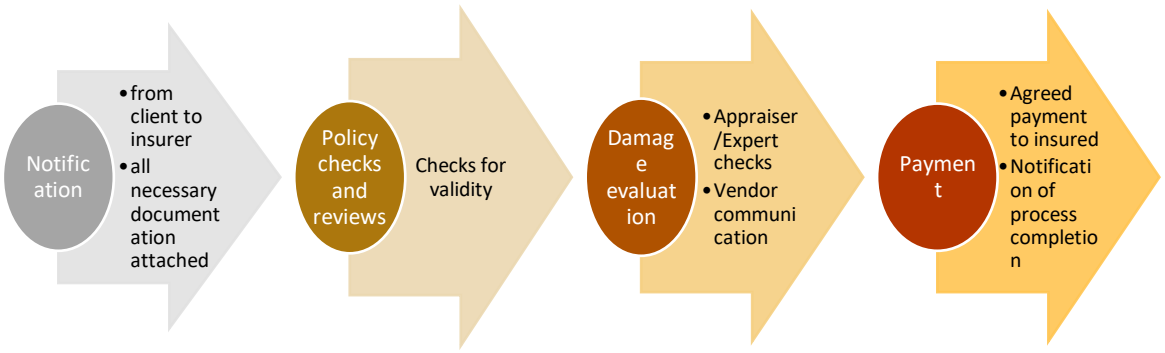
Since operational risks are a distinct risk category, the value of effectively managing them has increased considerably. The forms and manifestations of these risks keep on changing. For example, in recent years, cyber risk has become a critical operational risk for insurance regulators to address given the increase in cyber incidents, including data breaches, identity theft, ransomware attacks, and denial of service among other challenges (Basel Committee on Banking Supervision, 2004). As operational risk remains difficult to identify and assess, given that the causes are extremely heterogeneous, companies must constantly innovate on how to manage and mitigate them. Therefore, a robust operational risk management framework must be put in place by companies so as to deal with potential challenges.

Operational risk management (ORM) involves risk assessment, risk decision making, and implementation of risk controls to achieve acceptance, mitigation, avoidance and transfer of risk (Yang ,, 2017). In the last few decades, increasing complexities and volume of risks have led to the realisation that information systems ought to provide benefits for integrating risk management activities and optimising risk management performance (Breden, 2017). As such, operational risk monitoring should be integrated into the management of an organisation both in the policies, governance, and culture of the company as well as its structure and processes (Marshall, 2000). This will include institutionalisation of procedures to ensure properly managed risk, cohesion of goals through training of staff, developing risk and controls culture, and establishing dependency relations between roles and responsibilities. King (2001) states that these factors jointly determine the way in which an organisation operates, hence, failure in any of these factors will lead to operational risk.

1.1.2. Insurance Claims Processing

The claims processing procedure in Sanlam and most other insurers consists of;

Figure 1.1 Claims Processing



Notification: The client notifies the insurer of a claim request either through a walk-in to a branch, telephone, email or letter.

Registration/Capture: The branch representative or claims officer then begins the process of registering the claim request, verifying that the necessary supporting documentation is attached, cover is confirmed, and any other required checks (e.g., Anti-Money Laundering (AML) screening through various sanctions and other lists.)

Audit/Assessment: Once the initial officer has confirmed validity of the documentation and coverage, the documentation is then forwarded to the claims department for further processing. The forwarded documentation can be presented electronically, physically or in both formats depending on the internal procedures of the insurer. At this stage, further checks are performed by the claims team, and claims adjusters. This is to validate the claim request, claim amount payable, validity of damage (e.g. vehicle damage and amount needed for repair, spare parts, any third party injury bills or any other costs) are commensurate with the claim amount available/requested.

Majority of insurers both global and local face challenges at the audit/assessment stage with respect to fraud. Fraud is termed as claims extortion involving acquiring financial advantage through falsification of an actual position (Scwab, 2014). There are four main categories of insurance fraud that affect claims processing namely: internal fraud, policyholder fraud, intermediary fraud and insurers' fraud which can arise both internally and externally to the insurer (Akomea-Frimpong, 2016). Internal fraud involves commission of fraudulent

activities by an insurer employees while external fraud encompasses fraudulent activities by third parties (policyholder, and other stakeholders) in business with insurers.

Globally, insurers face "gargantuan losses running into billions stunting growth and financial well-being" (Akomea-Frimpong, 2016). Health insurance fraud suffers the greatest loss of approximately $40-60 billion a year in the US alone while in Kenya, fraudulent losses account for 40% of insurance claims paid (Akomea-Frimpong, 2016).

Payment: Once investigations and validity of a claim is concluded, the claim request is then forwarded to the finance unit to issue payment to the client. Relatively small sum payments can be lumped and paid quickly if they are below a defined amount (Mahlow, 2016). In comparison, standard claims and complex claims take a relatively longer time as there is closer inspections and necessary approvals either from senior management or external validators/auditors before they are settled. Payments are then released and depending on the amount, can be deposited into policyholders' accounts or mobile money wallets.

Closing/Archiving: Once the process is complete and payment initialized, the policyholder is informed through listed modes of communication of when to expect payment and amount payable. Depending on bank procedures and complexity of the claim, the average majority of claim requests are settled within 2 weeks to 3 months of notification.

The objective of claims process is to compensate the policyholder for covered incidents in the policy taken. The insurer's procedures in the claims process validate the request, authenticate it, and reimburse money to the policyholder, healthcare provider, or any third party as indicated by the claim. The insurer can also choose to reject the claim request if through the claims process it is found to be fraudulent or outside of policy terms.

At each given stage of the process, there can arise various operational risks. The likely operational risks to be of note include: Fraud (external or internal), inaccurate data entry, incorrect payment details, delays according to set timelines, and reputational damage in the event of poor customer service.

Operational risk monitoring entails; identification, analysis, and mitigation of the different categories of risks. Effective monitoring of operational controls within insurers ensures optimal internal and external client engagement and feedback (Siddiqui & Sharma, 2010), approval matrices designed for payments are always adhered to, and escalations are done

where key decisions are necessary. This translates to smooth process operations, increased customer feedback, growth in business volumes as insurers build brand image, reduction/elimination of costs due to efficiency, and an overall profit and insurer growth. The converse of lack of proper monitoring leads to direct economic losses such as; regulator penalties and fines, reputational damage, reduction in sales, legal proceedings against insurers, increased operational risk economical capital holding, loss of share price and market share leading to lack of investor confidence: that could result in hostile takeovers.

1.1.3. Overview of Insurance Sector in Kenya and Sanlam

This study concentrated on the Kenyan region and the Kenyan insurance industry. The Kenyan insurance sector is divided into General (55.2%), Life Insurance (27.6%), and Pensions (39.8%) where the General Insurance (GI) sector is the largest in size despite low market penetration (2.3%) compared to other key economies (Insurance Industry Release Report, 2021). Every year, The Insurance Regulatory Authority (IRA) updates their annual reports and claim ratios'. In Quarter one (Q1) 2021, the claims payment ratio for general liability claims increased to 9.2% (Q4 2020: 8.4%). The claims payment ratio for general non-liability claims decreased to 64.7% in Q1 2021 from 70.3% reported in Q4 2020. The claims payment ratio for the long-term insurance business increased to 73.7% compared to 73.1% observed in the previous quarter (Insurance Regulatory Authority Report, 2021). In order for companies to make a profit in the insurance industry, all paid premiums are allocated according to the expenses listed in the policy agreement. If majority of all paid premium to an insurer is retained over the 12-month period of majority of GI policies instead of payment in claims, the insurer is able to release these funds as profit generated. There are a variety of participants in the industry namely: customers, insurers, reinsurers, brokers, agents, banks and risk managers. The Insurance Regulatory Authority (IRA) sets and enforces the statutes regulating the industry. Aside from the IRA, The Association of Kenyan Insurers (AKI) and Insurance Institute of Kenya (IIK) act as secondary self-regulating authorities with key roles in accrediting, training, professionally educating and managing brokers, agents, and intermediaries. Kenya's total premium revenue for 2020, as listed by IRA, was Ksh.232.95 billion 56.2% of which was attributed to GI (Insurance Regulatory Authority, 2020) in comparison to a global premium income of USD 6,292 billion with 53.7% attributed to global GI companies. As at 2021, 56 insurance companies operated in Kenya (Insurance Regulatory Authority, 2021).

1.1.4. Sanlam Insurance Company

Sanlam Insurance Kenya is a subsidiary of Sanlam Ltd. a Pan-African financial institution based in South Africa. It provides individual, group, short-term and long-term insurance solutions. Sanlam holds 3% market share in General Insurance and 6% in long-term business (IRA, 2020) in Kenya. As per the 2020 IRA annual statistics report, Sanlam General Insurance paid out 2% of all industry claims made whilst Life insurance paid out 4% of industry claims made. However, the regulator offers no insight or reporting on any operational risks that the company faces or how they monitor risk and its management including operational risk management.

Sanlam Kenya has adopted technology to assist with claims administration and other back-office needs but is yet to implement advanced tools to better manage, and monitor risks inherent in the business. However, the company has implemented governance structures that enable it to adequately prepare and note any risks arising in the course of everyday business, including; Group risk management policies, risk appetites, and ERM frameworks, board committees on Audit, Actuarial and Risk functions providing assurance on risks facing the business, dedicated Risk and Compliance function, and ownership of risk & controls within the business (Sanlam, 2020).

1.1.5. Technology Usage in Monitoring Operational Risks

Insurers globally have generally been among the slowest to adapt to changing customer behaviour, digital disruption, and regulatory pressures. Competitive marketplaces are forcing insurers to refine their current strategy and operating models by implementing technological solutions. Further to this, various growth-related internal and external challenges such as low-interest rates, soft pricing conditions to technology advancements, and the expectations to deliver profitable and sustainable growth amidst these changing environments are some of the hurdles the insurers are facing. As a result, insurers and technology firms have had to innovate and collaborate extensively on a mission to reduce the problems named above. Some of these technological tools used extensively include predictive data analysis, artificial intelligence, Big Data, Machine Learning, IoT (Internet of Things), Chabot's and drones, among many others that have yet to show a profitable use case in the industry (Mitra ,, 2016).

Insurers and insureds are already adopting some of these instruments for their business purposes. The scope of adoption for insurers and insureds varies widely as a result of the different industries and portfolio of businesses these two distinct groups operate. However, Insureds and Insurers are more likely to employ some similar tools to improve; value chains, product distribution channels, customer services, client services, backend operations, and risk monitoring. Marsh, a well-known insurance and reinsurance broker as an example, has been working on a United Nations (UN) financed project to create modelling applications that include assessment of value at risk (VaR), Monte Carlo simulations and stress testing, and models of financial projections inclusive of test scenarios that can potentially negatively affect an insurer (Njegomir, 2011). Despite the above modelling being mainly utilised to identify, measure and monitor other insurer risks, they have been adopted to deal with operational risks.

Value at Risk (VaR) has been transformed to OpVaR that is contextualised using operational risk and creates a percentile loss distribution on losses or failures from operational risks (Barros, 2013). VaR measures the potential loss in the value of a risky asset or portfolio over a defined period of time given a confidence level of 95% (unknown, 2020). OpVaR can then be defined as the minimum potential loss an insurer will incur should any operational risk arise. This can be modelled using Monte Carlo Simulation that allows for building a useful distribution of losses for monitoring and making decisions about operational risk. Operational risks are slowly becoming the largest contributor to the total risk portfolio of an insurer, although some operational risks may be dominant while others require triggers in order to fully realise the scope of their effects (Mitra ,, 2016).

With increasing connectivity and internet penetration around the world, fraud, cyber and other technology risks are on the rise and there is still a distinct lack of understanding on the manner in which to address them. Other contributors to operational risks outside of an insurer's control include natural disaster, war, political strife, global warming, terrorism and so on, which may lead to increased operational risks outside of the control of technology. However, having robust technological monitoring of risks will enable adequate and timely response.

Blockchain Technology was first introduced in a published paper by Satoshi Nakamoto in 2008 and was the base for the introduction of his first peer-to-peer electronic cash system relying on cryptography (Bitcoin) in 2009 (Sarmah, 2018). It provided a solution to the

problem of currency duplication and double-spend (McKinsey, 2016). It gained notoriety due to its transparency, decentralisation, safety, and speed in settling payments for goods and services. Its decentralisation and cryptographic elements are key in ensuring that the technology is tamper proof.

Blockchain can be considered as an architecture of three layers; applications (which is the top layer), decentralised ledger (middle layer made up of a consistent and tamper proof global ledger where transactions are grouped into blocks and cryptographically linked), and Peer-to-Peer (P2P) network (bottom layer consisting of nodes and messages that can be built on any physical infrastructure) (Sarmah, 2018). It relies on four foundations to be effective: *consensus* – agreement of all participants to follow the same rules; *immutability* – permanence of records; *provenance* – knowledge of asset origination, owner, and time period owned; and *finality* – a single ledger for the whole network. It is a technology that allows creation and editing of transactional records managed by a cluster of computers (Neale, 2020). Similarly, there are different types of Blockchain; public, private, semi-private, sidechains, permissioned ledger, distributed ledger, shared ledger, fully private or proprietary Blockchains, and tokenized or token-less Blockchains.

However, since Blockchain Technology appeared on the global technology map, in the last 15 years, it has caused innovation and rapid evolution in the manner by which organisations work. It has created new business models, transformed previously inefficient methods, and created/improved product and service delivery value chains. By leveraging Blockchain technologies, insurers can dramatically reduce operating costs through automating manual tasks involving data entry in areas such as underwriting, claims, and reinsurance (Breden, 2017). This in turn has the potential to increase processing speeds, improve data quality, eliminate fraud, and provide real-time transaction transparency. 58% of surveyed executives and experts from the information and communication technology sector believe that 10% of global GDP will be achieved by the mid-2020s through the use of Blockchain Technology as per World Economic Forum (WEF). Similarly, a survey 'Blockchain in Insurance: Risk Not, Reap Not' (2018) states that, 86% of respondents affirmed the very important impact of Blockchain on the insurance industry, from which 54% predicted the transformation of the industry citing potential benefits in speeding claim process, simplifying and upgrading administrative processes, and record keeping offering more transparency in addition to fraud reduction (Mitra ,, 2016).

1.2. Statement of the Problem

Operational risk consists of failures resulting from people, processes, systems, and/or external events that remain difficult to monitor since the causes are extremely heterogeneous (Johnson, 2006). The existing methods of monitoring them are equally weak and easily manipulated to defeat the very purpose they are supposed to serve. Similarly, lack of adoption of new value-based technologies in the industry creates problems such as; fraud, data entry, verification errors and long processing periods on claims, rise of operation risk costs, and declining customer satisfaction. Crucial to note, the lack of capacity and leadership on these new technologies within the regulatory bodies also exacerbates the operational risks experienced in claims processing. (Simon-Kutcher, 2017) states, the main reasons pushing clients to change their insurers are costly pricing (29%), mismanaged claims (20%), cover not adapted to policyholders needs (16%) and premiums escalations without justification (7%).

Therefore, there is a need to develop a sound operational risk monitoring framework that extends well beyond the confines of formula-based quantification as is the case now and employs new technology within the claims processing. Moreover, lack of proper operational risk monitoring has led to direct economic losses such as regulator penalties and fines, reputational damage, reduction in sales, legal proceedings against insurers, increased holding of operational risk economic capital, drop in share price and market share leading to lack of investor confidence resulting in hostile takeovers. The likely operational risks of note include Fraud (external or internal), inaccurate data entry, incorrect payment details, delays according to set timelines and reputational damage in the event of poor customer service.

Dealing with operational risk entails identification, analysis and mitigation, and monitoring of the different risk categories. The operational risk framework should cover the company's business activities and should be an integral part of an efficient Enterprise Risk Management (ERM) framework. Therefore, an insurance firm's underlying operational risk in the claims processing should thoroughly review the claims processing activities in order to identify and estimate the framework input requirements. Blockchain Technology can be used to assist firms to track the claims processing activities in order to flag out any potential operational risks. Moreover, it can promote accuracy and transparency of claims transactions through increasing an insurers' ability to identify, monitor, and mitigate

operational risks associated with claims transactions while increasing customer engagement and satisfaction.

Furthermore, the monitoring of the operational events around the claims processing including acquiring, processing, sharing, and securing operational loss data that will lead to making real-time decisions (Omasete, 2014). This will translate into smooth process operations, increased customer feedback, growth in business volumes as insurers build brand image, and reduction or elimination of inefficiency costs. Despite the potential of Blockchain Technology to tackle the problems stated, limited study has been undertaken in Kenya to determine how to monitor operational risks in claim procedures. Similarly, there is limited study that exists to analyse how different types of operational risks are monitored, or frameworks in use for monitoring operational risks in claims processing and studies on developing a framework based on Blockchain Technology for monitoring operational risks within claims processing in insurers. It is in this backdrop that the current study seeks to develop a framework on integrating Blockchain Technology in monitoring operational risks arising from claims processing.

1.3. General Objective of the Study

The purpose of this study was to develop a framework for monitoring operational risks in the claims processing in the insurance firms utilising Blockchain technology.

1.3.1. Specific Objectives

i. To examine the claim processing operations in Sanlam;
ii. To analyse the operational risks indicators within the claims processing operations and approaches of monitoring them at Sanlam insurance;
iii. To review how information communication technology has been utilised to monitor operational risks at Sanlam insurance; and
iv. To propose an operational risks monitoring framework that uses Blockchain technology in the claims processing at Sanlam insurance.

1.4. Research Questions

i. What are the claim processing operations in an insurance firm?
ii. What are the operational risk indicators associated with the claims processing and approaches of monitoring them at Sanlam Insurance?

iii. How has information communication technology been utilised to monitor operational risks at Sanlam Insurance?
iv. How can Blockchain technology be integrated in the claims processing so as to monitor the operational risks at Sanlam Insurance?

1.5. Significance of the Study

This study was expected to be significant to insurance companies, the general public and the insurance regulators as it would offer valuable contributions from both theoretical and practical perspectives. Theoretically, it would provide a general understanding of operational risk monitoring practices and their effect on financial profitability as well as develop a framework for Blockchain technology to be used in monitoring claims processing. The study is expected to enable insurance companies to record risk, increase the speed, accuracy and transparency of their claims processes using the Blockchain technology framework. This should translate into better performance, business growth and maintenance of competitive advantages. Apart from benefiting the insurance companies, the general public will benefit from the study through improved insurance services in the form of reduced premiums and better monitoring of risks in order to inform actions taken (especially with regard to fraud).

The study would also be useful in government policy making institutions/commissions through the Ministry of Information, Communication and Technology, and independent institutions by putting in place policies that allow insurance industry regulators and stakeholders to access the Blockchain framework as a starting point for bringing digital technology that fosters regulator-industry collaboration on insurance practices.

Embarking on this research aims at contributing to the body of knowledge by developing a framework for Blockchain technology in monitoring operational risks in claims processing in all insurance firms in Kenya.

1.6. Scope of the Study

In view of the study, the research takes into consideration the insurance industry in Kenya. Since, technology adoption is inherently influenced by the context in which it is to be adopted, Zhengchuan and Yufei (2009) further considered that claims processing function is dependent on the organisation policies and procedures (Girling (2013). The study was

scoped to a case study of Sanlam Insurance and data collection done in a span of two weeks. The study was limited to development of a framework for monitoring operational risk in the claim processing using Blockchain Technology.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

This chapter presents literature review with regard to monitoring operational risks in claims processing within insurers, discusses existing technology used to monitor operational risks, and presents the case for the integration of Blockchain in claims processing. The chapter discusses theoretical foundations which comprise theories supporting the study as presented by other scholars and researchers. The chapter is organised thematically in line with the study objectives and presents the empirical literature review, research gaps, as well as the conceptual framework of the study.

2.2 Theoretical Framework

A theory is a generalisation about a phenomenon that explains how or why the phenomenon occurs (Avolio, Yammarino & Bass, 2009). The study is anchored on three theories namely; Structural Contingency Theory, Agency Theory and Risk Management Theory.

2.2.1 Structural Contingency Theory

Structural contingency theory is an extension of the contingency theory that states that there is no superior way of doing something that can be replicated in all circumstances for effective management of an organisation (Flynn ,, 2010). Structural contingency theory therefore offers an explanation on how an organisation should operate by linking the strategies and decisions it pursues with its contingencies which include organisation structures, processes, environment, performance and technologies (Bouriche, Wilson and Kishk, 2021).

The theory further supports the argument that organisational performance comes from fitting the organisation characteristics to key contingency factors related to a particular challenge an organisation faces (Donaldson 2001). Moreover, an organisation whose characteristics fit with the contingencies will outperform those that do not fit (Miles, 2012). The contingency fitting focuses on the effect of an independent variable over the dependent variable through a moderating factor. Further, the theory suggests it is possible to reject one way of doing things to adopt an alternative way based on the circumstances.

Through holistic configuration which is a form of analysing organisation fit, the overall internal coherence of a set of organisational attributes, or simultaneous interdependencies among variables that are subject to multiple contingencies within Sanlam were achieved (Cao, Wiengarten & Humphreys, 2011). This formed the basis for understanding the interplay between different variables and processes involved in the claims processing.

By applying the structural contingency theory in this study, it helped in understanding the role of the principals and the agents in comparison to the goals of the company. Furthermore, to achieve an organisation's goals will greatly depend on; employee's ability to achieve it, level of technology in the organisation, structure and task at hand and the support given by the company owners (Mutegi, 2013). The goal of most private organisations like Sanlam is to maximise returns on investment and create value for shareholders. This can be achieved by a keen consideration of both internal and external contingencies. Internal contingencies involve the task to be achieved, whether it is structured or not, the kind of resources to be used and levels of uncertainty and interdependence. In this particular case, these internal contingencies can be considered as operational risk categories and their levels of correlation. The external contingencies include the political forces, technological effect, government regulations and the general public. All these contingencies have an effect on insurance firms especially so where the general public expects to see faster, efficient, and easier ways in which to have their claims processed.

This theory therefore provided a foundation understanding the various contingencies considered in the proposed framework and also the basis for proposing an alternative way of monitoring operational risks associated with claims processing through the adoption of Blockchain technology.

2.2.2 Agency Theory

Agency theory offers an explanation on the relationship between the party giving authority (principal) and the party receiving the authority (agent). Principals in this capacity delegate tasks and some decisions to agents in order for the agents to complete these tasks in the best interest of the principal (Davis, 2016). The principal in the agency theory and in the context of this study refers to the owner of the company or shareholders while the agent refers to the management, who is expected to take control over the management of the owner's

assets. The differences between the interests of the principal and agents often may result in a conflict of interests. Sometimes conflicts may arise when the managers want to maximise their levels of expectations against the wishes of the owners. On the other hand, the company owners may wish to maximise profit margins thereby creating conflicts when the managers' expectations are not aligned to the company owners (Abbas ,, 2021). Once such conflicts arise, the principals will then need to give attention to conflict resolution through incentives (Mitchell & Meacham, 2011).

Jensen and Meckling (1976) notes that causes of the agency conflicts can be categorised under the following motivations: a) Moral hazard which is the dishonest behaviour by the actors at the expense of other parties' interests. For instance, the company management may choose the most suitable investment options for themselves and not the most profitable option for the company; b) Earning retention whereby the management shifts towards maintaining stable company income levels whereas the company owners would prefer a higher cash distribution through internal investment options; c) Risk aversion where the management would prefer to make safe investment decisions within their ability and they avoid investment decisions they consider likely to increase the company's risk even when the option is not the best choice for the company; d) Time horizon where the management pays attention to the cash flow statement based on the predetermined project timeline. This leads to biases in decision making in favour of short-term projects which may have higher accounting returns instead of long-term projects with greater net present value for the company.

Sanlam as a company is potentially faced with these four scenarios and through the agency theory the interaction between principal and agent in the present research problem is underscored. Building on the proposition by Abbas ,, (2021) of tackling such conflict situations through auditor monitoring and guidance in pointing out to the managers the interests of the company owners', to facilitate them in making decisions aligned with the interests of the company owners'. Furthermore, agency theory underpins the procedure of risk management as a response to conflicts between administrative motivating forces and shareholder interests, this theory was critical in understanding how the possible risks that may arise in the claims processing in Sanlam insurance company could be associated with different players.

2.2.3 Risk Management Theory

Risk management theory is sometimes referred to as the risk management model. Risk Management theories were first developed after World War II but did not have published materials until the early 1960s from Mehr and Hedges in 1963, and Williams and Heins in 1964 (Dionne, 2013).

The risk management theory is based on three concepts: utility, regression and diversification (Ajupov, 2019). The utility concept was proposed by Daniel Bernoulli in 1738 to guide the decision-making process whereby people were expected to pay attention to the size of the effects of different outcomes in selecting alternatives. The concept of regression also called the rule of regression function has been used in varied circumstances to calculate probability of risks and making predictions based on identifiable business risk factors. Diversification concept is more of a strategy that has been used to guide institutions to intelligently arrive at investment decisions that minimises deviation from maximising the rate of return.

The risk management theory has been applied in financial institutions to distinguish between two varieties of deposit banking risks: temporary or fixed-term, and resource risks (Rusanov, Natocheeva, Belyanchikova, & Bektenova, 2017). The fixed-term deposit risks are associated with threats of early withdrawal of funds by depositors from banks earlier than the agreed fixed term. The resource risks are associated with the failure of both the creditors and depositors in giving the bank their temporarily free funds either through making a term deposit, or buying securities issued by the bank hence starving off the bank of funds. The two risks have inherent characteristics of claims in the case of insurance since they are sometimes dramatic and unexpected due to factors like emergence in the market of a more attractive offer from other banks, inadequate actions of banking supervisory and regulation authorities, undermining the confidence of depositors in the banking system institutions, deterioration of the bank position, and loss of reputation (Ajupov et al 2019). These factors have also been pointed out to be the influencers of some claims made in the insurance industry.

Wenk (2005) notes that risk management incorporates; identification, assessment, and prioritisation of risks followed by coordinated economical application of resources to mitigate, monitor, transfer, and control the probability or impact of unfortunate events or

maximise the realisation of opportunities. Corvellec (2009) also notes that risk matters can be addressed from within the organisational *modus operandi* through contracts, selective view of responsibility and dialogues with employees. Haubenstock (2003) however argues that effective risk management can bring far reaching benefits to all organisations, whether large or small, public or private sector. Studies by Gollier (2003) state that these benefits include, superior financial performance, better basis for strategy setting, improved service delivery, greater competitive advantage, less time spent firefighting and fewer unwelcome surprises, increased likelihood of change initiative being achieved, closer internal focus on doing the right things properly, more efficient use of resources, reduced waste and fraud, better value for money, improved innovation, and better management of contingent and maintenance activities.

The significance of this theory as pointed out by Dorfman (2007) is that it describes cost effective operational risk management as creation of a well-defined embedded risk management practice, co-signed through top-to-bottom management dialogue. Sofiane, (2020), indicates that the application of risk management theory could offer a framework through which an organisation can lower its likelihood of known risk events occurring. For instance, having a risk monitoring policy/framework will allow the organisation to manage operational risks in an integrated manner that considers threats at each level of the entire organisation (Drennan & McConnell, 2007). Therefore, for an organisation to thrive it will need to formulate policies on risk management strategy, and organisational objectives and develop predictive models that lead to optimal performance and reduced risk exposure. Hence, the application of the risk management theory in this study was central in understanding the potential risks in Sanlam, the strategies used to manage them, the responsibilities assigned to different employees in case a particular risk occurs, and how the risks are monitored. It is through these parameters that the proposed framework for monitoring operational risks in claims processing is structured.

2.3 Empirical Literature

2.3.1 Operational Risk management

The Basel Committee on Banking Supervision (2004) defines operational risk as the risk of loss resulting from inadequate or failed processes, people or systems or from external events. Similarly, the Global Association of Risk Professional (GARP) distinguishes

operational risk management as the qualitative assessment of operational risks. The Basel Committee further identifies some of the categories of operational risk to include; unauthorised activities, unethical employment practices and workplace safety, theft and fraud, internal security breaches, and business or market practices, product flaws, and selection, sponsorship & exposure.

Operational risk indicators are an important tool within operational risk management. They facilitate operational risk management activities and processes, including: risk identification; risk monitoring and control assessments; and the implementation of an effective risk management and governance framework.

In an operational risk context, a risk indicator, commonly known as a key risk indicator (KRI), gives a metric that provides information on the level of exposure to a given operational risk which the organisation has at any particular point in time (Coleman, 2009). KRIs are an important tool within risk management and are used to enhance the monitoring and mitigation of operational risks and can be used to gauge effectiveness of systems and controls put in place by an organisation. If a risk indicator falls outside of its normal range, it can indicate a possible operational issue and provide a basis for penalties, or positive incentives to reduce agent-principal problems (Tripp, 2004).

Operational KRIs enable risk managers to identify conditions that may result in losses and act upon them before actual losses are realised; the metrics also act as indicators of changes in the risk profile of a firm. They therefore play an important role as a way to facilitate changes in strategic objectives, review of existing structures within the organisation, review of risk appetite and policies, and allow for the organisation's management to reassess operational risk management activities and their efficacy. This includes risk identification; risk and control assessments; and the implementation of a governing risk appetite, risk management and governance frameworks.

Scandizzo (2005) states that risks can be mapped to the business activities in which they are prevalent and where key risk factors and drivers can be identified. This results in complex rich qualitative assessment giving clear indications to which faulty parts of the process can be changed in order to lower overall operational risk exposure.

The complex operational functioning of insurance companies has led to the emergence of operational risks that can affect the business operations of insurance companies. Operational

risks are very difficult business risks that affect both the insurance company and the customers. These operational risks arise from imperfection of business processes and technology systems. In previous analysis of operational risks in a company, tracing of the information systems stability, customer requirements, and errors in internal control were treated separately. The need to consolidate and standardise the analysis of operational risks has led to the development of a framework called Solvency II.

Risk management is core in strategic management and corporate governance of any organisation. It is also central in strategic and operational decision making in an insurance company. The growth of operational risk management is a regulatory driven approach which requires managers to determine the level of risk capital (Acharyya, 2012). However, the success of the implementation process of operational risk management depends on the availability of information and expertise of employees in the insurance company. The key human resources groups involved in risk management in an insurance company include internal auditors, risk modellers, compliance and business managers.

The main goals of risk management in an insurance company are provision of protection from potential events that manifest operational risks; alleviating the effects and impacts that may arise from operational risk; and establishment of controls due to the occurrence of operational loss events.

The structure of the process of operational risk management is integral to the broad process of risk management in the insurance company. It therefore must be effective, safe and economical. Since operational risks are specific, the activities that lead to them must be accurately defined and functions for managing them in terms of roles and responsibilities of the stakeholders across the organisational structure in an insurance company clearly spelled out. This is also dependent on the establishment of an efficient and reliable system of risk management that is accurate and timely in terms of information on all the relevant data, and software support for the implementation of an adequate model for managing operational risk.

Successful operational risk management is largely dependent on the identification of key processes and the types of operational risk arising from these processes, relating to people, communication of products and systems. Therefore, the adoption of a company-wide definition of operational risk by all employees of the insurance company is critical in

understanding and identifying a risk event. Correct risk identification forms the basis for the development of monitoring and control of operational risks. The identification of operational risk considers the structure of the insurance company, the quality of human resources, organisational changes and turnover per employee (internal factors), and other external factors that can affect the achievement of the objectives of the insurance company. After the identification of the operational risk, management of the identified risk may involve risk mitigation, risk-taking, risk avoidance or sharing, and risk transfer.

2.3.2 Monitoring Operational Risks

Dhanushkoti and Coates (2006) define monitoring as the regular and ongoing collection and analysis of information to track progress against set plans and check compliance to established standards. In the insurance sector, specifically the claims department, monitoring makes use of available information on claims processing in order to make comparisons both internally and externally. Krishnan (2010) states that the existence of a reliable monitoring system or framework is extremely significant for evaluation of claims processing.

Asokere and Nwankwo (2010) posit that monitoring of operational risks in claims processing can be done by identifying areas that need to be adapted or changed. This would enable insurers to identify trends and patterns, adopt strategies and inform decisions on actions to be taken. Crawford (2007) states that the process of monitoring can involve tracking the use of inputs and resources, the progress of activities, and the delivery of outputs. Insurers can also create more robust models of operational risk management and monitoring which can become better as more data is collected on identified Key Risk Indicators (KRI).

KRIs are relevant in monitoring and in forward-looking analysis of operational risk to complement statistical analysis where there is insufficient data (Finlay, 2004). KRIs can be specific causal variables or proxy drivers of events and/or losses related to operational risk. It can be quantitative or qualitative; objective or subjective but, in order to be useful, must link to one of the key risk drivers or better yet to one of the mechanisms generating an operational failure (Scandizzo, 2005).

The KRI can be classified into three categories according to Tripp (2004). Exposure related – these are volume-based indicators that allow measurement throughout processes likely to

incur operational failure. These however lack dynamic measurement to notice changes in loss rate. Loss related indicators – these measure events associated with operational losses and are considered lagging indicators hence insufficient alone. Cause-related indicators – these measure factors identified as drivers for operational losses and are leading indicators. Leading indicators are usually tough to identify as they rely on a causal relationship between indicator and associated operational loss, and are complex but valuable.

According to Diggelmann (2011) KRIs are critical predictors of unfavourable events adversely impacting organisations. They enable the user to monitor changes in risk exposure and give a method for setting early warning signs. This can then enable an organisation to report risks, prevent crises, mitigate and transfer them before they fully crystallise.

Monitoring indicators are therefore metrics used to monitor identified risk exposures over time with relevant data performing this function considered a risk indicator. Shiller (2006) states that a metric may be considered to be a risk indicator when it can be used to measure; the quantum (amount) of exposure to a given risk or set of risks, the effectiveness of any controls that have been implemented to reduce or mitigate a given risk exposure and how well insurers are managing their risk exposures (the performance of their risk management framework). Expressed slightly differently, this implies that an insurance firm will typically make use of three different types of indicators: risk indicators, control effectiveness indicators and performance indicators (Vaughan & Vaughan, 2008). This study however, focuses on the risk indicators.

The risk indicators should therefore be understood to be the predictors of adverse events that are likely to negatively impact the organisation. In general, some of these indicators can impact the organisation once the environment changes. Therefore, the operational risk indicators are likely to be dependent on the organisation's environment and hence not static. A clear mechanism of identifying the indicators and where in the claims process they apply should be robust enough. The general criteria for establishing the operational risk indicators involve the following steps: understanding the cause-effect relationship between the organisation's goals and some root cause factors; understanding the relative significance that each of these root cause factors has on the overall achievement of the goals; and creating a system that collects high-quality data about these indicators. Some of the indicator data points in the claims processing include errors, regulatory changes, economic downtime, staff turnover, customer satisfaction among others.

2.3.3 Operational Risks in claim processing in USA

Within the US industry, banks and insurers have in the past had operational loss events greater than $50 million, some of which indirectly affected a few other industry players due to contagion risk (Cummins, 2012). Investigating using network analyses, allows players to note which firms within the industry are likely to encounter severely negative effects from contagion risks and can aid in risk mitigation measures (Eckert and Gazert, 2019). This was especially noted during the financial crisis of 2007/08. One such insurer that experienced extensive losses was AIG which resulted from CDS (Credit Default Swaps) written by the insurer. This points to a failure in the control environment within the insurer and adequate risk management.

Major lessons have established that operational risks should include; corporate culture, training, experience, ability to cooperate, and willingness to obey rules since human factors grossly affect operational risks (Chofaras, 2004). Similarly, the lack of comprehensive operational risk databases negatively impacts risk-based pricing and appropriate operational risk-based capital allocation.

Within claims processing, the operational risks arising are categorised as per Basel II operational risk categories. One of the major findings in Chernobai (2011) research is that operational losses are a consequence of a poor internal control environment, poor governance, and accountability/oversight.

2.3.4 Operational Risks in claim processing in Europe

In Europe and the UK operational risks are thought to be difficult to accurately determine and are often inseparable from other risks (Manning, 2005). Therefore the main approach chosen is to first identify operational risks in claims processing and thereafter attempt to quantify the insurers appetite threshold for each of the said operational risks.

One of the largest insurance market franchises is Lloyd's of London which holds a capacity of 62 underwriters with capacity of £221 million of which 60+% is in property and casualty with over half of that as reinsurance (Manning, 2005). Similarly, 45% of their business sits in the US while 39% in the UK and Europe. This therefore exposes Lloyds to a diverse set of operational risks.

Manning (2015) posits that Lloyd's (among many other insurers) in the market have adopted the Basel definition of operational risk with a slight change that includes both direct and indirect operational losses. Operational risks have a bearing on other risks faced by any underwriter. Poor controls in claims processing can result in market risk or enhance credit risk for an insurer. This also includes operational risk arising from people and their management.

Subjective understanding of risks by individual underwriters can lead to significant losses where pricing is below defined levels for new risks, lack of understanding of risks but an underwriter accepts the class of business, or inadequate controls in underwriting business leading to losses. These risks are therefore prevalent when claims are made and can lead to regulatory sanctions, fines, or loss of operating licence.

Therefore the ability of a European/UK insurer to identify risks and loss events will allow it to make appropriate changes to its systems and controls, thereby reducing operational risk failure. Another key observation is the need for data collection and analysis in order to truly quantify and monitor operational risks. Within EU/UK insurers, the majority of high frequency low impact risks are accounted for daily but low frequency, high impact risks are at the tail end of most models of operational risks (Manning, 2005). A truly standardised model for measuring, monitoring, and mitigating operational risks is difficult due to distinct internal approaches within insurers to governance, operational risk identification, differing control frameworks, level of technology adoption within insurers (i.e. claims processing systems), and interpretation of operational risks.

Spanish insurers have over the years struggled with the lack of an external database nor developed expertise in standardisation of operational risk data to identify and predict operational risks. However, due to the availability of health insurance operational losses database, operational risk and statistical techniques were used to develop models useful to risk management (Barros, 2012). Barros (2012) in his research utilised an external database of operational risk insured losses, concerning claims and incidents reported by 21 Spanish health insurers between 1998 and 2008. This database contained 1200 claims of insured losses worth €10.7m from general insurers. A broker reviewed the data to ensure the losses were covered under policy hence producing a consistent and homogeneous set of data which was then used for further analysis. The findings of this research showed that internal databases are necessary and the manner in which they are treated is key for operational risk

modelling under Solvency II and future modelling of operational capital charges (Barros, 2012).

2.3.5 Operational Risks in claim processing in Africa

As indicated in section 1.1.2 operational risks in the insurance industry could be events and actions or inactions that may lead to capital loss. Therefore, organisations must guard on them by consistently monitoring and managing their operational risks (Ohando, 2015). It therefore becomes imperative that insurers seek to monitor levels of operational risk exposure as a formal process and a fundamental business requirement. Risk, control, monitoring, and performance indicators provide information on operational risk and any potential future losses, making it possible to identify and monitor elevated levels of operational risks early on and to take appropriate measures.

However, due to the lack of a structured way to share data between different insurers on operational risk losses, there is a distinct lack of operational databases that can be utilised to quantify operational risk.

2.3.5.1 Operational Risks in claim processing in Sanlam Insurance Company

Sanlam Kenya has employed various methods to try to quantify, measure, mitigate, and monitor operational risks. The methods used include; robust governance policies cascaded within the organisation, board committees on audit and risk functions within the organisation, and fully employed enterprise risk management framework including documented processes used to identify, measure, monitor, and mitigate operational risks.

Within claims processing, one method used extensively is risk and control registers that set out risks per process performed within the claims department according to their standard operating procedures, their correlating operational risk categorization as per Basel II, and controls employed to mitigate these risks. The business unit then assesses itself using inherent risk (frequency multiplied by severity) before control measure is applied and after control measures are applied. This is done monthly to ensure any gaps are spotted and any potentially catastrophic operational loss is dealt with before it crystallises. The claims department also does a self assessment of departmental functions relating to operational risk and the risk department also assesses the claims unit on a quarterly schedule to ensure controls meet the risks on which they are applied to.

Bi-annually, the risk and compliance department also performs an overall audit of operational risk using a risk appetite document that states the company's risk appetites and thresholds as set from the parent company. Table 1.1 shows an extract of the risk appetite assessment tool in use at Sanlam Insurance Company.

Table 1.1: Risk Appetite Framework Sanlam Kenya (example)

Risk Type	Risk Appetite Statement	Measurement Indicator	Threshold	Actual	RAG
Brand Risk	Sanlam brand is not to be associated with any negative transactions, activities, and events	1. Number of adverse media reports 2. Number of regulatory investigations	0	0	
Fraud Risk	Incidences of internal or external fraud will not be tolerated and immediate action will be taken on the offending party if discovered	Number of reported fraud cases Number of investigated fraud cases Number of prosecuted fraud cases	0 ALL 0	4 4 0	
…	…				

2.3.6 Comparative Operational Risk Monitoring

2.3.6.1.1 Case of EU and UK

Insurers in Europe are, by regulation, required to adhere to solvency II directives on measurement and capital required in order to ensure optimal exposure to operational and other risks. Solvency II aims to provide a standardised principle of measuring and managing operational risk. This has transformed the manner in which operational risks are perceived. Recent trends in globalisation, technology advancement, and competitive requirements have transformed views of operational risk and the far-reaching consequence of inadequate management. Organisations looking to be successful in an environment of uncertainty

should give emphasis on innovation, increased risk tolerance and striving for a culture of change acceptance and adaptation in order to thrive (Torre-Enciso, 2013).

Gazert (2009) further states that the impact of operational risk on insurers can be measured under risk-based capital assessment of Solvency II directives. Operational risks are considered to be complex to measure and assess. Approaches like operational value at risk (OpVaR) (without considering diversification effects) can aid in the study of the impact of dependencies between operational risk, loss distribution, and among others (Gazert, 2009). Risks are then measured across claims management, policy administration and particular risk management. Advancing information systems will lead to using richer and much more complex models to efficiently allocate capital in risk modelling (Torre-Enciso, 2013). OpVaR provides information on minimum potential loss suffered within a given time period and certain level of statistical confidence (Torre-Enciso, 2013). This can then be used to perform monitoring exercises.

In the UK, banks have collaborated on a confidential database that enables them to access accurate data for evaluating operational risk. There are also worldwide emerging proprietorial databases such as OpVaR and Basel II/III that have also aided in the measurement and monitoring of operational risk (Tripp, 2004). However, insurers in the UK lack this sort of collaborative database that can be used to determine operational risk exposure accurately. One method insurers employ to overcome this is use of statistics on claims data issued from regulators, but this still lacks the true accuracy needed to determine and monitor operational risks.

Due to the extensive networks such as the actuarial professional body UK, insurers are still able to pull together data from different sources which enables better estimation of operational risks. For an effective Blockchain operational risk monitoring process, extensive data collection will be required for effective quantification of operational risk indicators and monitoring of operational risk. Tripp (2004) also states that having a comprehensive set of risk indicators along with corresponding escalation triggers will enable an effective risk reporting process. This will entail having a good database of losses on operational failure, quantitative targets for improvement and good techniques for predictive analysis.

2.3.6.2 Case of Tunisia

In a regional analytical study done by Hermit (2012) based on a list of key risk indicators, analysis was performed to understand the link between KRIs and operational risk events that exist in the Tunisian insurance sector. It was noted that since each event risk was associated with a set of key risk indicators, it became easier for insurers to create faster data analysis for organisational operational risk. Events considered to be under "clients, products and business practice" and problems associated with "execution, delivery and process management" were mainly correlated with "omissions and actions and inactions of employees" whilst "Business disruption and system failures" arose from "lack of internal control" and "actions and inactions in management process". "Internal and external fraud" were linked to key indicators such as "governance" and "changes in market conditions" (Chernobai, 2009).

Hermit (2012) study evaluated operational risk as per the four levels of granularity in the Tunisian insurance industry namely: activity (auto, causality, life, etc.), sub process (underwriting, claims, etc.), operation (registration, regulation, etc.) and elementary task (mailing a cheque, etc.). Each business line was then associated directly or indirectly to operational risk. Measurement of operational losses was assessed using questionnaires capturing frequency and the severity was then assessed through industry experts.

2.3.6.3 Case of Kenya

As indicated in section 1.1.2 operational risks in the insurance industry could be events and actions or inactions that may lead to capital loss. Therefore, organisations must guard on them by consistently monitoring and managing their operational risks (Ohando, 2015). It therefore becomes imperative that insurers should seek to monitor levels of operational risk exposure as a formal process and fundamental business requirement. Risk, control, monitoring and performance indicators provide information on operational risk and any potential future losses, making it possible to identify and monitor elevated levels of operational risks early on and to take appropriate measures. They permit statements to be made on trends and can serve as indicators in early-warning systems. Examples of key operational risk indicators include staff fluctuation rate, days of sick leave, hours of overtime, number and duration of system failures, internal audit findings, frequency of complaints, and wrong account entries (Omasete, 2014).

Operational risk monitoring could also be seen in the broader context of operational risk management. In Kenya, some companies that have managed their operational risks by instituting clear and sound strategies have registered significant growth (Chepkoech & Rotich, 2017). A study by Njuguna (2017) indicates that adherence to clear written policies and procedures is key to the management of operational risks in Kenya. The study also recommends the following strategies for effective management of operational risks, establishment of operational manuals, establishment of internal system controls for detecting potential frauds, conducting random spot checks and internal audits and benchmarking and adoption of technologies.

2.4 Technology Utilisation in Monitoring Operational Risks

Over the last few decades, insurers have been adopting technology in order to improve efficiency and reduce expenses. In the last decade alone, the majority of insurers have shifted focus to acquiring and building technology allowing for better and larger data collection and management. The current focus of claims processing technology is ensuring a system that offers speedy assessment whilst maintaining robust service delivery. Several claims processing technology vendors exist in the market today offering a range of services that allow for recording of claims, ability to approve and validate, escalation to senior management, AML screening of clients, and integration to other systems in the claims processing cycle. This integration includes links to banks, assessors, adjusters, medical and smart card providers, and mobile money services (Stein, 2006).

However, there is scope for operational risks in claims processing that can be measured and monitored through the use of technology, the available systems require large proportions of manual data entry which are often riddled with inaccuracies. Neale (2020) states that for insurers to survive long-term, their ability to innovate is important with a majority of insurers today who are focusing on automating and improving the claims process. Current improvements involve telematics, augmented reality, drones, and other remote inspection technologies.

According to Sinisia (2015) the general insurance industry adequate risk quantification and understanding insurers require rich data done through use of telematics data allows for combination of mileage, speed, location, time, total duration of trip, G-force, (extrapolated from telematic devices) to improve billing methods through alignment of individual price and risk more precisely. Jayanthi (2019) discusses the use of computer-based methods to

facilitate inspection of vehicles to detect damage and problems emanating from previous repair and guide in estimating cost of repair for direct and indirect damages while Soles (2014) discusses the use of impact detection system using sensing devices for identifying damage related to structural integrity. These particular devices use electromagnetic readings to produce damage data. Jayanthi (2019) further proposes a system that utilises augmented reality to measure damage to the body of vehicles and therefore determine appropriate payable claim payments. These systems can then be used to monitor operational risks arising from inaccurate claim amounts based on structural integrity readings, losses from poor repair and inspection of vehicles, frequency of losses from particular third-party's poor repair services, and any fraudulent activity.

According to Catlin, Paliath and Segey (2014) meeting clients' needs at any time of the day, and without delay, is a priority for most insurance companies. But this is an almost impossible task for a human workforce. Artificially intelligent technology, like robo-advisors, step into the breach. Properly deployed robot-advisors can handle routine or repetitive insurance operations that do not need human intervention, like collecting customer data, processing queries, and even underwriting new policies. This technology could eventually replace brokers and automate most duties, while still offering customer support similar or better than that provided by humans. Other "Robo-advisors" include insurance advisors and asset management by automated systems. Though a relatively new innovation in insurance, robo-advisors are already standard practice in wealth management and financial services. Once trained, they run according to a set script (Desyllas & Sako, 2014). Robo-advisers could then be employed by insurers to monitor operational risks arising from process inadequacies.

One documented example of an employed robot adviser is Lemonade, an American top-rated fully digitised insurance company that deploys its services almost entirely through virtual assistants. Initially, it utilised AI assistants - Jim and Maya -to perform simple operations but in 2017, Jim successfully executed a theft claim in just 3 seconds. In Europe, French insurer, Natixis Assurances, has taken the step to entrust contract termination and email processing to a robot capable of carrying out the equivalent amount of six-day labour of a staff member in a single night (Businesswire, 2020). More and more insurers are considering the benefits of entrusting certain manual tasks to artificial intelligence in order to improve accuracy and speed. This will in-turn reduce or all-together eliminate operational risks arising from inaccuracies in capturing data and maintaining policyholder information.

It would also reduce costs associated with the need for physical labour, costs related to fraudulent activities, and improve customer experience.

According to Deloitte (2020) the establishment of a system based on the technologies of artificial intelligence (AI) is not risk-free and there are concerns related to AI. Some of these concerns include the insured's preference to maintain human contact, finality of decision making, back-office administrative, recurrent or accounting tasks, concerns regarding job security, and operational risks resulting from robot malfunction, failures, bad programming and misinterpretation of data.

Gamification is another insurance industry innovation that is rapidly gaining traction and considered a powerful tool to activate massive growth within areas of historically low performance (Sheehan, 2020). Though gamification is not a new technology, many insurers have recently started to adopt it as a way of creating more customer-centric digital solutions. Due to its relatively low implementation cost, gamification is currently one of the prevailing IT trends in insurance (Hunter, 2011). Gamified elements foster closer relationships with clients, for example, gaming tactics can work on advertising life insurance to millennials on known, popular interactive digital platforms (Zichermann & Cunigham, 2011). Operational risks related to employment practices and workplace safety can then be monitored through gamified elements (Grove, 2011). Risk associated with employee relations, diversity, and inclusion in the workplace can be monitored and addressed through incentives for employees to produce, learn, and become more resourceful. One such example is the use of applied gamification to the claims scheduling process to drive engagement in the insurance industry (PwC, 2020).

Ross, Sebastian, Beath, Mocker, Moloney and Fonstad (2016) argue that the growth of the Internet of Things (IoT) has been a game-changer for businesses and consumers' alike , pushing customer's attitudes towards rapid results as the norm. IoT is primarily a connected chain of devices: mobile phones, printers, computers, cloud services, and any other related technology. The consequence of which is the elimination of paperwork and reduction of the tedious delays caused by the physical exchange of documents. IoT technology will enable faster customer engagement to assess claims, facilitate prompt data review and processing by agents, allow for simultaneous inter-departmental access to data to accurately adjust premiums, and on-board new clients (World Insurtech, 2020). However, the increased

creation of sensitive data on networks will need sufficient monitoring to ensure no risk of breach.

Big data is changing insurance in significant ways. Companies are employing AI-enhanced predictive models using data available internally and externally to reveal profitable trends and patterns. Wargin (2020) states that without big data and machine learning for process automation, marketing and customer interaction will be less productive leading to losses attributed to competitive pressure. The potential benefits of big data such as better data collection, and automation will positively impact operational risk management. General insurers are documented as using data analytics and software engineering to assess risks related to motorists to better design products, improve customer selection, and monitor exposure to risk limits (Schwab, 2017).

There are however some major challenges to automating processes using machine learning such as limited knowledge of AI throughout industries, and the increased need for extensive processing power to run algorithms and collect significant amounts of data and creation of scripts to process tasks (Swiss Re Institute, 2020). As more and more insurers adopt automated claims processes, operational risks related to people will be eliminated as those related to systems and processes are likely to become more prominent. It is noted that implementation of insurance technology will begin with the simplest and least costly solutions and progress to more complex and costly projects (Neale, 2020).

2.4.1 Blockchain Technology in Insurance Sector

Blockchain is a distributed, open source, and community-based ledger that ensures accountability and transparency (Gera, 2020). It relies on four foundations to be effective: *consensus* – agreement of all participants to follow the same rules; *immutability* – permanence of records; *provenance* – knowledge of asset origination, owner, and time period owned; and *finality* – a single ledger for the whole network. It consists of individual transactions cryptographically coded to form a chain of blocks where each block is a cryptographically signed real-world transaction requiring multiple party validations that then create a permanent record of transactions. As a distributed ledger, Blockchain is a common database of validated and encrypted transactions adhering to agreed-upon common terms and rules (Quincy Analytics, 2018).

Blockchain technology is likely to revolutionise the insurance sector (Grima, 2020). For instance, the adoption of the technology will facilitate and speed up operations in the insurance firm. Grima (2020), describes Blockchain technology to be a Distributed Ledger Technology, which consists of technologies that collects, stores, distributes and facilitates exchange of some information/data between private and public users. It therefore consists of modules and distributed ledgers that bring together applications that allow for an audit trail of all operations performed by peers without the need for a centralised authorization and it exists on the entire computing network in an organisation (Pratap 2018).

Grima et al (2021), posits that research on Blockchain technology is drawing a lot of interest on how it can be used to solve challenges related to insurance problems in various sectors. In their article they describe how Blockchain technology has been used to address aspects of Digital Operational Resilience Act (DORA) and how Blockchain has been used to tackle challenges of effectiveness of a digital system application used in the operations of the European insurance market sector in terms of DORA.

With the Blockchain, contracts are embedded in a digital code and stored in some transparent and shareable databases with immutable properties (Iansiti and Lakhani, 2017). Pratap (2018) identifies some important attributes of Blockchain in the insurance contracts and operations context. Some of these important attributes include, transparency, time-efficiency, precision, security, reliability, data storage, cost savings, and trust (Grima et al, 2021). Patrap (2018) further notes that the Blockchain technology has unlimited potential that can satisfy the needs of regulators and can allow for proportionality in terms of risk management and compliance requirements.

According to Grima , (2021) some of the benefits and characteristics of Blockchain technology that can be useful to the insurance industry include immutability of data, which means that data cannot be changed (Crawford 2020); ability to automate the claims process by integrating salespeople to prevent fraud; transparency of transactions that improves the detection of fraud attempts; data verification and preservation so that it may be used over times since there is continuous consumer engagement and satisfaction; can promote creation of new insurance products relevant to improved means of exchanging sensitive documents through creative solutions; implementation of shared central data storage system that promotes joint management of the data; secure data and information storage that prevent

data loss; robust authentication and verification of users; and promotion of look up to historical transactional states.

A number of researchers note that for an information system to be effective in addressing the needs of an IT risk management system, it must have certain characteristics. These characteristics include flexibility and adaptability; integration and alignment with processes; trustworthiness and reliability; accuracy and consistency; and verifiability (Napitupulu, 2016; Tan, 2016; Qatanani and Hezabr 2015). Other aspects that are important of an information system are ability to ensure confidentiality, integrity, authorization, authentication, nonrepudiation, and cybersecurity (Napitupulu, 2016; Shagari, 2017). Blockchain technology is considered to promote the creation of a system with all these characteristics.

One key tenet to monitoring operational risk is the availability of relevant data that can be used to develop key risk indicators. Blockchain Technology has the capability to make monitoring operational risk easier and more accurate due to its *immutability* and capacity for large amounts of data. Likewise, there will also be a corresponding increase in security, increase in efficiency, decrease in fraud and record sharing (Neale, 2020), and a decrease in costs both within the claims process and in monitoring operational risks.

In designing an appropriate application within Blockchain, insurers will be able to make decisions on whether to have public, private or hybrid Blockchain that will allow for external nodes to verify data (using the *consensus* foundation) (Sayegh, 2018) and the use of smart contracts in implementation of operational risk monitoring. Blockchain potential to eliminate inefficiencies from intermediaries and allow for programmable direct interaction with policyholders will permit the use of smart contracts programmed to release payment, and alert users on breach of operational risk limits. Within the claim process, smart contracts can be deployed throughout to notify, assess, or pay claims and collect data applying the foundation of *finality*.

Existing insurance systems have achieved a certain degree of automated processing. However, due to the lack of a single trusted information source of different transactions, the majority of these systems suffer from performance bottlenecks. Additionally, generic insurance systems require manual interactions across different transaction processes, hence resulting in slow processing, and lengthy payment settlement time (Christidis &

Devetsikeiotis, 2016). This has resulted in poor detection of fraudulent claims of which implementation of Blockchain and the application of its foundations of *immutability*, and *provenance* would handle efficiently (Watanabe ,, 2016).

2.4.2 Technology Adoption in Claims Processing in Kenya and Sanlam

Shultheis and Sumner (1995) note that IT has changed the nature of the industries in which firms operate with respect to products and services offered. IT has increased delivery speed, production economics in which Sanlam operates, and concurrently increased globalisation and accessibility within Kenyan insurers (Gitonga, 2010). IT offers Sanlam Kenya the scope to improve and fully automate its business processes which improves competitiveness, allows access to new market opportunities, and allows for exchange of real-time information between organisations, stakeholders, and customers.

Some key adoption of IT with respect to claim processes are in; requiring biometric registration and authorization for claims; automating the claim process from notification, registration, assessment, payment, and archiving; and sharing information relevant to fraud within the industry to the regulator. Biometrics and unique identification coding have been employed within Sanlam and the insurance industry to fight fraud through eliminating multiple identities and fake documentation (Swapnil, 2018).

However, ineffective IT governance and control is likely to be the main cause of operational problems. This includes lost business, damaged reputations, weakened competitive position, and inability to meet deadlines, failed or aborted projects, budget overruns and poor returns on investments (Nyakomitta, 2009).

Some large and complex claims are likely to require manual intervention and IT systems may not be optimal or flexible enough to capture all the intricacies of the claims (Kiana, 2010). Additionally, Sanlam like other insurers has interfaces with service providers that are not linked directly which results in poor claims tracking and lack of appropriate information to make management decisions. Kiana (2010) also noted that despite the existence of good IT systems, these systems were underutilised leading to inefficiency and poor customer satisfaction. Similarly, IT systems should be such that they allow for industry sharing of information in order to reduce incidences of operational risks arising from fraudulent claims.

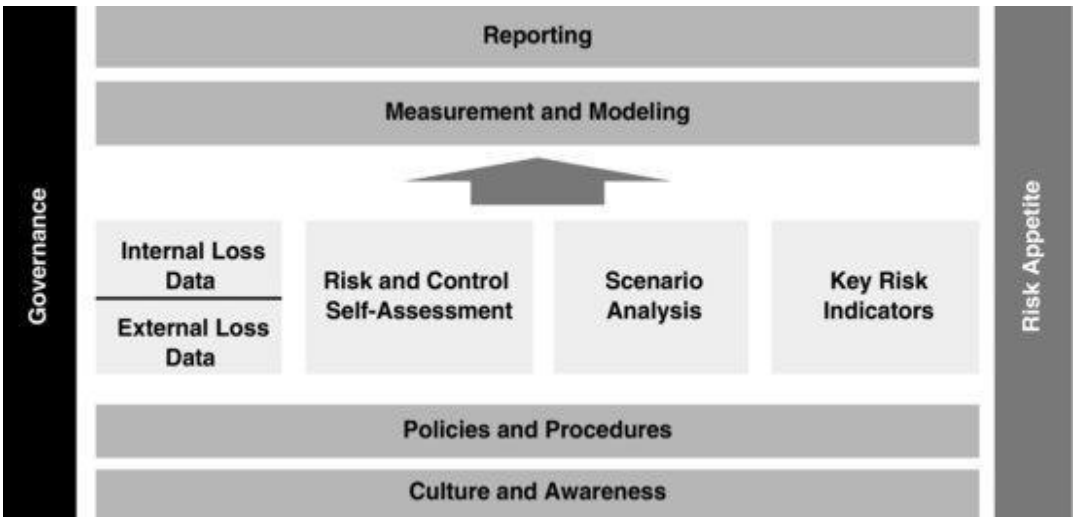
Sanlam Kenya, has employed technology within its claims processing to automate the entire process however no specific system is in use for monitoring operational risks. There are robust governance structures in place that will allow for integration of IT in order to monitor operational and other risks. The company however relies on manual monitoring of operational risks including estimation of operational economic capital to be held as a hedge against any operational risk occurrence. However, the company is a subsidiary of the largest pan-African insurer and has the capacity to introduce a decentralised operational risk monitoring tool that could leverage all the advantages of IT.

2.5 Key Components of an Operational Risk Monitoring Framework

Operational risk frameworks were first introduced in the early 1990s through the committee of sponsoring organisations of the tread way commission (Kirikkaleli ,, 2020). They considered that the frameworks should have internal control systems composed of five integrated components; control environment, risk assessment, control activities, information and communication, and monitoring activities (Pakurár ,, 2019). At the time, operational risk was considered residual risks and hence there was no specific framework in place to; identify, measure, treat, and monitor them.

In general, operational risk frameworks have the same building blocks which include: loss data collection, risk and control self-assessment (RCSA), scenario analysis, and key risk indicators. These then feed into governance, policy and procedures creation, and internal risk appetite (Girling, 2013). Figure 2.1 illustrates the general structure of an operational risk management framework.

Figure 2.1: Operational Risk Framework (Girling, 2013)



Governance, policy and procedures creation, culture and awareness, and internal risk appetites formed the foundation and pillars upon which operational risk management frameworks were built on. The governance component defines the roles, and responsibilities of the risk function as well as managing the risk and committees that oversee key decisions on risk management. It ensures a formal structure for risk escalation and transparency in operational risk management. The policies and procedures elements of the framework provide clear, actionable and measurable guidelines to be followed. They are aimed at eliminating ambiguity, increasing autonomy of business units, and reduced regulatory supervision. On the other hand, the risk appetite provides a threshold and rating of operational risk that a firm may be able to absorb or the limit within which a risk control mitigation could be triggered. Further, it is considered embedding a risk management culture within the organisation will allow the business to consider risks before any decision making at all levels within the enterprise creating a more robust approach to operational risk management.

The framework guides that data collected on both internal and external operational risk losses should be mapped to key operational risks. In the insurance sector this could include; data entry errors, procedural errors, incorrect payments, invalid claim requests, and client complaints. These will then be used in root-cause analysis and automated risk mitigation strategies. Data collected from internal sources needs to be valid and reliable and done within effective governance. This data is essential in creating an operational risk measurement approach like the Risk and Control Self-Assessment (RCSA). RCSA involves; Identification of risks and controls in order to develop effective and efficient

control and mitigation strategies for any elevated key operational risks. On the other hand, data collected from external sources is important in creating operational risk models, risk and control self-assessments, and scenario analysis. Scenario analysis considers high impact and low frequency events in order to identify catastrophic operational risks that will lead to the collapse of an organisation. It involves stressing the operational risk framework and aids in application of innovative solutions.

As discussed in section 2.3.1, KRIs are used to monitor identified risk exposures over time by collecting relevant data on the functional units considered. In the framework, a risk indicator can be used to measure; the quantum (amount) of exposure to a given risk or set of risks, the effectiveness of any controls that have been implemented to reduce or mitigate a given risk exposure and how well insurers are managing their risk exposures - the performance of their risk management framework (Shiller, 2006).

Measurement and modelling, and Reporting are considered the output of the operational risk management framework. Operational risk modelling can be performed using advanced measurement approaches to combine the operational risk indicators to single points of failure or areas of constant errors. These can then be modelled to prioritise operational risks management initiatives to address them. Reporting components of the framework provides a mechanism to communicate the outputs from the process levels to the various functional departments involved in the management of the operational risks. The key to success in operational risk reporting is consideration of relevant, concise but precise delivery of information that allows for the management to make key operational, strategic, and organisational decisions.

2.6 Claims Processing Flow

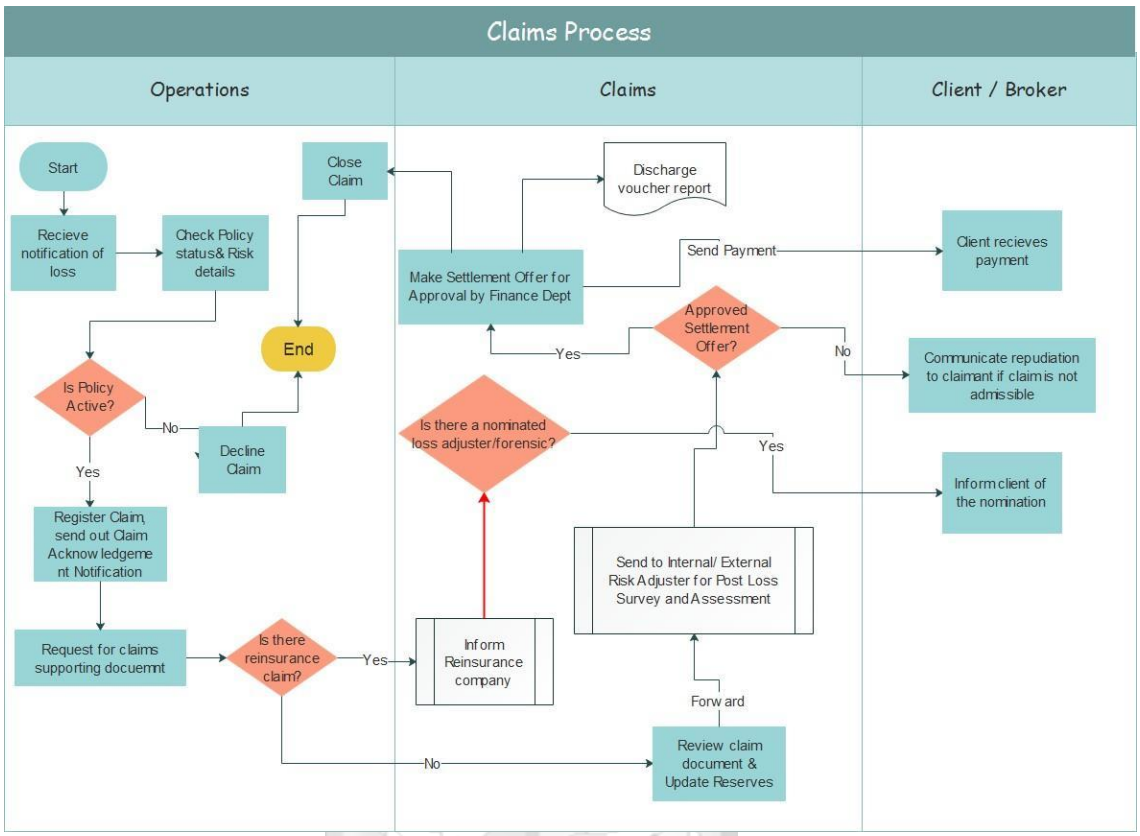
Claims processing is one of the critical stages of claims handling within an insurer. It is the point of interaction between the insurer and policyholder, defining customer relationships for the majority of insurers globally, and a major contributor to an insurer's success (Shiu, 2014). In the European insurance markets, annualised growth of total benefits-and-claims spend is more than 4% (€350 billion) yearly. Insurance claims processing is now a much longer, and more time-consuming process with several inefficiencies including ageing technology, increasing process complexity, and a rising number of fraudulent claims (SAS, 2012). In order to achieve their goal of higher levels of operational efficiency and better process effectiveness, insurers are seeking to implement modern claims systems or enhance

their existing claims systems, leverage advanced fraud detection technologies and innovate around self-service and straight through processing. The ultimate test or objective for insurers is in a consistent, yet flexible and fair manner, transparent, accurate and timely, as well as a secure and compliant claims handling process (Mehari & Aemiro, 2013).

All claims processing in the majority of global and local insurers undergoes the same claims procedure in five main processes namely: notification of the claim by insurer, verification, assessment, payment, client notification (Mahlow, 2016). Currently in Kenya, the claim process begins as a manual process where the claimant presents documentation and claim forms either via email or physically. The claims officer then reviews the documentation and notifies claimant if he/she is required to provide further documentation for the process to continue. The claims officer then confirms validity of policy, up-to-date premium payments, any pending policy loan payments, and if the peril is covered under the insured's policy.

Majority of insurers both global and local face challenges at the audit/assessment stage with respect to fraud. Fraud is termed as claims extortion involving acquiring financial advantage through falsification of an actual position (Scwab, 2014). There are four main categories of insurance fraud that affect claims processing namely: internal fraud, policyholder fraud, intermediary fraud and insurers' fraud which can arise both internally and externally to the insurer (Akomea-Frimpong, Andoh & Ofusu-Hene, 2016). Internal fraud involves commission of fraudulent activities by an insurer's employees while external fraud encompasses fraudulent activities by third parties (policyholder, and other stakeholders) in business with insurers. Globally, insurers face gargantuan losses running into billions stunting growth and financial well-being (Akomea-Frimpong ,, 2016). Health insurance fraud suffers the greatest loss of approximately $40-60 billion a year in the US alone while in Kenya, fraudulent losses account for 40% of insurance claims paid (Akomea-Frimpong ,, 2016).

Figure 2. 4: Claims Process Flow (Akande, 2018)



Once documentation and initial reviews are complete, the claims officer then initiates system claim requests on whichever vendor the insurer uses in order to initiate, track, assess, and pay claims. Relatively small sum payments can be lumped together and paid quickly if they are below a defined amount (Mahlow, 2016). In comparison, standard claims and complex claims take a relatively longer time as there are closer inspections and necessary approvals either from senior management or external validators/auditors before they are settled. Payments are then released and depending on the amount, can be deposited into policyholders' accounts or mobile money wallets.

At this stage, potential operational risks arise from incorrect or invalid information provided, irregular activity by the claims officer, fraudulent claims request and/or supporting documentation. The claim processing technology in place can be considered inadequate as it requires manual input and physical documentation.

2.6.1 Categories of Operational Risks in Claims Processing

Measurement of operational risk at each of the stages in the claims processing procedure involves a quantified approach which questions system integrity, identifies sources of

threats whether external or internal, identifies vulnerabilities whether in the procedure itself or in the claims recording system. Historically, proper measurement of operational risk in monetary terms has been difficult due to inability to quantify monetary loss from people or processes. This has affected the ability of an insurer to adequately monitor operational risks in monetary terms. Having a system or framework in place would allow for a continual monitoring of operational risk and would ultimately reduce the burden on an insurer arising from operational costs (Girling, 2013).

The Basel Committee on Banking Supervision (2004) defines operational risk as the risk of loss resulting from inadequate or failed processes, people or systems or from external events. Similarly, the Global Association of Risk Professional (GARP) distinguishes operational risk management as the qualitative assessment of operational risks. The Basel Committee further identifies some of the categories of operational risk to include; unauthorised activities, unethical employment practices and workplace safety, theft and fraud, internal security breaches, and business or market practices, product flaws, and selection, sponsorship & exposure.

2.6.1.1 Unauthorised Activity

These are recognized as losses caused by law violations, breach of contract, internal rules and procedures. Additionally, loss from internal acts involves at least one internal individual giving rise to unauthorised activities which refers to events where the perpetrator engages in a deliberate act of wrongdoing, but intends or expects to benefit all parties at least in nominal terms. It can also be referred to as trading misdeeds. Types of activities that arise from unauthorised activities include intentional failure to report transactions that may constitute fraud by a computer or fraudulent registration, insider trading, front-running, intentional manipulation of/with documents, erroneously conducted operational activities (intentional), trading above limits, misuse of vested responsibility, poor determination and presentation of position.

Insurers have employed segregations of duties between front office and functions in charge of supporting, verifying and monitoring transactions (e.g. operations, settlements, legal, finance, risk control, compliance and internal and external audit, hereafter called “control and support functions”) to monitor unauthorised activities. Insurers should consider whether an appropriate physical segregation of functions would enhance the implementation of rules and roles associated with claims processing (e.g. front office staff

should not have physical access to back-office IT systems, printers and documentation in the absence of back-office staff) and if this would mitigate unauthorised activities. Insurers should then consider and quantify if system segregation of duties such as initiator and approver roles or systems segregation in terms of different systems for the various steps in claims processing could further reduce operational risks arising from unauthorised activities.

2.6.1.2 Theft and Fraud

These are losses caused by acts aimed at personal financial gain from both an internal and external act intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/discrimination events. Activities generated from theft and fraud consists of credit fraud or worthless deposits, theft extortion, embezzlement or robbery, misappropriation of assets, malicious destruction of assets, forgery, cheque kiting, smuggling, account take-over or impersonation. Other additional examples of theft and fraud activities include; tax non-compliance or wilful evasion, bribes or kickbacks, insider trading (not on firm's account), unauthorised funds transfer, wire fraud and money laundering.

Monitoring of losses by insurers arising from activities linked to theft and fraud are carried out through conducting investigation on legitimacy of claim requests, ensuring there exists adequate systems or physical security controls allowing unrestricted access and fraudulent supporting documentation (CGMA, 2012). Similarly, studies indicate that an effective fraud risk management framework enables insurers to have controls preventing fraud from occurring, detect fraud as soon as it happens, and respond effectively to fraud incidents when they occur (ACFE, 2010).

Insurers should therefore analyse possible sources of fraud and define anti-fraud measures, taking into account fraud exposure resulting from market-related activities. Depending on the size and type of exposures to fraud within the market-related activities, monitoring fraud can then be part of a daily control process within the market area, while other fraud monitoring activities may be performed on a less frequent but regular basis.

2.6.1.3 Internal Security Breaches

These are losses caused by unauthorised access to data, malicious manipulation of data, damage or deletion of data, and unauthorised use of IT systems by internal or external parties. Majority of cybercrime activities are as a result; misuse of IT systems, theft of

information loss, hacking, manipulation of files and programs, web page defiance, inadequate passwords and firewall breakdown.

Monitoring of such losses can be performed through appropriate design, implementation, and maintenance of information systems ensuring a high level of protection in claims processing activities. Access to data resources should be monitored through the use of proprietary software formally endorsed by senior management in order to automate claims processes. Periodic reviews of access requirements and systems should then be updated as often as necessary in order to prevent unauthorised access. Additionally, compliance with rules should ensure that assigned functions match authorised access and should also prevent access to information systems for fraudulent purposes.

2.6.1.4 Employee Relations

Losses arising from deceitful acts of employees, convention of health or safety laws or agreements, fraudulent payment of personal injury claims, or from diversity/ discrimination events is an operational risk arising from employee practices and workplace safety. Activities that involve employee relations include; compensation, benefit, termination issues, organised trade union activities (industrial action - strikes, picketing), hostile environment, wrongful termination, harassment libel/slander/defamation, employee illness, breach of non-compete and improper discharge.

Monitoring of losses arising from activities related to employee relations can be through appropriately developed, implemented, and examination of policies and procedures relating to leave requirements and staff movements. Tracking should therefore be carried out if staffing changes happen between front, middle and back offices or IT and potential risks stemming from a change in positions should be counterbalanced by appropriate control procedures. Hirsh and Cha (2015) argue that losses can be caused by gender, sexual orientation, race, age, religion, or nationality discrimination of employees.

Monitoring can then be approached through workplace policies, coupled with diligent reviewing processes, and will make for not only a suitably diverse workforce but an open and accepting workplace culture (Kmec, Hirsh & Skaggs, 2016). Capturing data staff recruitment will aid in developing a complete history of the insurer's effort in promoting and maintaining its policies (Kanhai & Ganesh, 2014).

Other sources of loss include breach of data confidentiality or code of conduct, violation of client's privacy, lack of transparency, erroneous/unlawful/negligent use of confidential data, unauthorised trading practices (aggressive sales), and account manipulation in order to create fictitious operations, concealing losses, unapproved access to accounts, and nondisclosure of sensitive issues.

2.6.1.5 Business or Market Practices, Product flaws, and Selection, Sponsorship & Exposure

Business or Market Practices are losses arising from violation of anti-monopoly regulations, improper trading or market practices, market manipulation, insider trading (on firm's account), engaging in unlicensed activities, violation of anti-money laundering law, failure to comply with regulatory framework in force, improper advertising, copyright infringement, professional negligence and client discrimination. Monitoring can then be done through adverse media reports and any issued regulator sanctions or requirements on the business.

Product flaws are losses caused by errors in products, services, models, product defects, ambiguous or punitive contract clauses. Whilst selection, sponsorship & exposure are losses caused by errors in selection of clients, in analyses of clients' needs or overstepping exposure limits. Monitoring activities can then be performed through evaluation of client data, and checks on adherence to policies and risk limits. The use of technology can then be leveraged in ensuring that contracts, and policy documentation are fully adhered to reducing exposure to operational risk.

Product flaws are losses caused by errors in products, services, models, product defects, ambiguous or punitive contract clauses. Whilst selection, sponsorship & exposure are losses caused by errors in selection of clients, in analyses of clients' needs or overstepping exposure limits. Monitoring activities can then be performed through evaluation of client data, and checks on adherence to policies and risk limits. The use of technology can then be leveraged in ensuring that contracts, and policy documentation are fully adhered to reducing exposure to operational risk.

2.7 Research Gaps

Kenyan insurers face massive gaps in the existing technology's ability to comprehensively identify, assess, and monitor operational risks. Although insurers have adequate information on any risk management activity, there is still a lack of an efficient means of

storage and proper document retention necessary for monitoring operational risks in claims processing (White, 2005).

Chudgar (2013) examined risk management in India using existing literature and found that prevention of fraud risk was possible through the creation of risk benchmarks; identification of vulnerable areas, compliance with applicable laws and regulations, formulation a risk policy, and ensuring efficiency and effectiveness of the existing claims procedures and their continual improvement. However, the study lacked comprehensive literature on how monitoring of operational risk can be accomplished in claims processing through adopting technology.

Generally, the majority of studies conducted on risk monitoring failed to give conclusive insights on integration of Blockchain Technology in monitoring operational risks in claims processing. According to Mwashi (2017) these studies gave general recommendations on automation, general improvement of information systems, regular employee training and fraud detection, prevention and reporting; establishment of a fraud department, adoption of advanced IT systems, ensuring strong internal controls and the establishment of an effective code of conduct as good practice for claims processing (Nyaga, 2018). However, there is scarcity of research in the Kenyan insurance industry with regards to Blockchain Technology leveraged as a means to monitor operational risk in claims processing.

The current study sought to design a claims processing framework built on Blockchain that will allow for effective and continuous monitoring of inherent operational risks within the claims process. It utilised the immutability property of Blockchains as a pillar to monitoring operational risks. The objectives of the proposed framework would be; to accurately detect operational risk using a decentralised digital repository and to monitor the operational risks within the claims process.

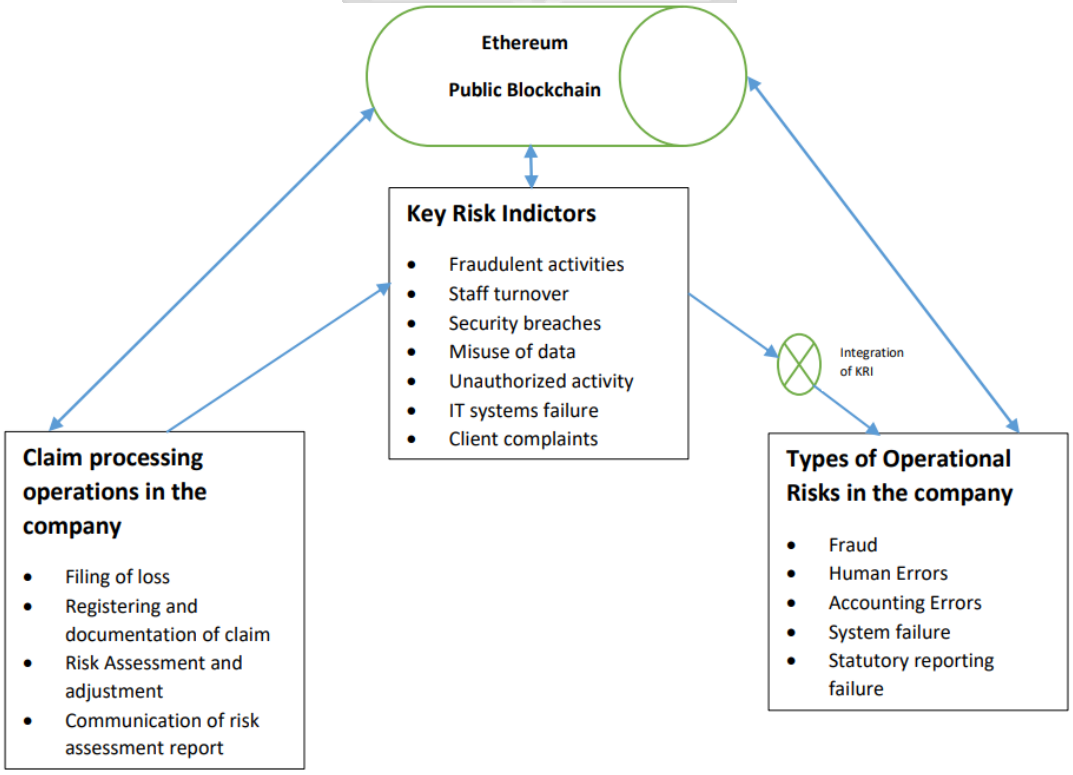
2.8 Conceptual Framework

As discussed in section 2.3.1, the success of operational risk management is dependent on the identification of key operational processes and the types of operational risk arising from these processes. The type of operational risks is also influenced by the kind of operational risk indicators which are associated with the operational processes in the claim processing. To effectively monitor the potential risks, effective systems involving both people and technology will be needed. Figure 2.3, shows a conceptual framework on the key

components that can be considered in the development of a framework for monitoring the operational risks in an insurance company. The conceptual framework assumes the consideration of the internal and external factors that can influence the operations in the claims processing. Every claim processing operational activities performed within the insurance company will be recorded in a directly accessible distributed database powered by the Ethereum Blockchain which possesses the immutable properties. Furthermore, everyone including the claimants is allowed to connect to the Blockchain and can transact through it with all transactions recorded in a secure manner.

The integration of Blockchain technology in monitoring operational risks in claims processing consists of key risk indicators that can be used as indicators of risks in claims processing. The key risk indicators act as the input variables that are fed into the proposed predictive model for analysis in order to flag out potential operational risks. The predictive model is built on the Blockchain technology so as to provide a mechanism of ensuring immutability of the operations once it has taken place. This also supports integrity of data during the claims process flow. Upon passing an event based on the input process, the predictive model under the Blockchain gives an output as a potential flag of the operational risk based on the input risk from the data feed into the framework.

Figure 2. 5: Operation risk monitoring conceptual framework



Operationalization of Variables

Operationalization of variables provides a means of transforming abstract concepts into clear measurable observations. It therefore involves mapping the variables to respective indicators or proxies. Table 2.1 shows how the study variables were measured.

Table 2.1: Operationalization of Variables

Research Objectives	**Variables**	**Indicators/Proxies**	**Data collection**	**Data Analysis**
Objective 1: To examine the claim processing operations in insurance firm	Claim processing operations	Filing of loss Registering and documentation of claim Risk Assessment and adjustment Communication of risk assessment report	Interview	Content Analysis
Objective 2: To analyze the operational risks associated with the claims processing operations and approaches of monitoring them at Sanlam insurance	Operational Risk indicators	Fraudulent activities Staff turnover Security breaches Misuse of data Unauthorised activity IT systems failure Client complaints	Questionnaire	Descriptive
Objective 3: To review how information communication technology has been utilized to monitor operational risks at Sanlam insurance	Information communication technology used to monitor operational risks	IT systems in use Levels of automation	Interview Questionnaire	Descriptive Content analysis

Objective 4: To propose a framework for monitoring operational risks that uses Blockchain technology in the claims processing at Sanlam Insurance	Framework for monitoring operational risks that uses Blockchain technology	Types of operational risks ➢ Fraud ➢ Human error ➢ Accounting eros ➢ IT System failure ➢ Statutory reporting failure	Framework design using Blockchain network architecture	Framework Analysis

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

This chapter presents an explanation on how the study was conducted resulting in the designing of the proposed framework for monitoring operational risks that uses Blockchain technology in the claims processing at Sanlam Insurance. It offers a description of the research design, the data collection and analysis methods adopted. The proposed Blockchain Technology framework seeks to provide a means of monitoring potential operational risks in the claims processing thereby enabling the management to take corrective measures.

3.2 Research Philosophy

A research philosophy is a framework that guides how research should be conducted based on ideas about reality and the nature of knowledge (Collis & Hussey, 2014). The two main research philosophies are positivism and interpretivism. These philosophies represent two fundamentally different ways that we as humans make sense of the world around us. In positivism, reality is independent of us and researchers can therefore observe reality objectively. Positivism claims that the social world exists externally and that its properties should be measured through objective measures, where observers must be independent from what is being observed. Since there is just one reality, this reality can be expressed by the variables and measured reliably and validly (Onwuegbuzie, 2012). Therefore, the researcher should focus on facts, locate causality between variables, formulate and test hypotheses (deductive approach), operationalize concepts so that they can be measured and apply quantitative methods (Easterby-Smith , 2012).

In interpretivism, reality is seen as highly subjective because it is shaped by our perceptions (Collis & Hussey, 2014). It assumes that generation of new knowledge can be achieved through subjective approaches. Rossman (2014) proposes a number of ways through which realities can be interpreted and new knowledge generated through experiences. This therefore calls for the adoption of qualitative research methodologies where experts are involved in providing the study data where deductions can be made from. This research study is underpinned by the positivism research philosophy. Positivism, as a research paradigm, seeks to solve major practical problems and discover precise causal relationships through statistical analysis (Kim, 2003).

The concept of operational risk monitoring using Blockchain Technology is an aspect of risk management through technology. Therefore, the conceptualization of operational risk monitoring using Blockchain Technology in claim processing in the insurance firm implies that the theoretical basis of the study would be from the risk management using technology. This confirms the deductive model adopted in the study since operational risk monitoring is an element of risk management.

In this study, the researcher assumed that there are some realities which exist in the insurance business involving claim processing that may need the application of Block-chain Technology in monitoring operational risks. The existing realities can therefore be expressed by the experts working in the insurance company and thus the study adopted an interpretive research philosophy.

3.3 Research Design

Research design is described as the logical guidelines that show how a study will be carried out (Saunders, Thornhill & Lewis, 2014). It can also be referred to as the general strategy used to integrate the various components of a study so as to develop a coherent and logical guideline for conducting an investigation into the research questions. It can therefore be seen as the blueprint of conducting the study and constitutes the elements of data collection, analysis and interpretation. Because this study focuses on the formulation of a framework for monitoring operational risks using Blockchain Technology in the claims processing and measuring levels of risk indicators, a mixed research design was adopted. Specifically, structured questionnaires and semi-structured interviews were used in data collection and both quantitative analysis and qualitative analysis were done.

Since, the claim processing operations are institutional and organisational structural dependent, the issue under investigation is therefore considered contextual. Therefore, the study adopted a case study method. According to Baxter et al, (2008) a case study method facilitates the exploration of a real issue within a known context using various data sources. Further, explanatory and exploratory designs were used in this study. Explanatory research was considered because it provides timely details where a small amount of information exists. Exploratory research was also considered because it is inexpensive, highly interactive and open-ended in nature (DeCarlo, 2015).

The research design adopted offered the researcher control on how potential input variables interplay based on the existing claim processing procedures so as to develop an adaptive framework. The general indicators of the operational risks outlined in chapter two aided in the development of the mechanism for flagging out the potential operational risk in a claim processing in the context of the selected insurance firm.

3.5 Target population and Sampling frame

According to Zhengchuan and Yufei (2009) technology adoption and assimilation by the organisation is contextual involving the unique characteristics of the organisation. Therefore, understanding the factors that would influence the utilisation of Blockchain Technology in organisation requires in-depth contextual analysis of the organisation characteristics on its preparedness to adapt to the technology. The study therefore used a case study focusing on Sanlam insurance company specifically the claim processing operations.

The target population constituted all employees of departments directly involved in the claims processing at Sanlam Insurance and have a higher direct exposure to operational risks. The department considered included Risk & Compliance, Internal Audit, Finance, Claims, Underwriting, and Premium Administration departments. The allocation of the number of people in each of these departments was arrived at through random selection and by seeking their consent to participate. According to Sekran (1992) assertion that sample sizes larger than 30 and less than 500 are appropriate for most research, the researcher used census technique as the sampling strategy since the study was a case study involving a single insurance firm. In total 48 respondents were involved in the study who constituted all the employees in the target departments at Sanlam Insurance directly involved in claims processing. The target respondents distributed across the departments considered are presented in Table 3.1.

Table 3. 1: Target Departments and Respondents

Target Departments	**Interview Respondent**	**Number of other officers per department who respondent to Questionnaire**

Risk & Compliance	Head of Risk & Compliance	3
Internal Audit	Head of Internal Audit	5
Finance	Finance Manager	8
Claims	Claims Manager	8
Premium Administration	Premium Admin Manager	8
Underwriting	Underwriting Manager	8
IT	Head of IT/Manager	8
Total	**7**	**48**

3.6 Data Collection

Since the research was a case study, it relied largely on primary data. Semi-structured interview and structured questionnaire data collection methodologies were used. Specifically, for the quantitative data, a structured closed and open-ended questionnaire was used to allow room for in-depth query on study constructs to get adequate data from the respondents. It was the primary data collection tool. The questionnaire was self-administered in following the COVID-19 containment protocols.

Semi-structured interview protocol was used to provide better means of collecting quality information due to its ability to allow for high engagement with the respondents (Marshall and Rossman, 2014). It was also used in this study to generate confirmatory results and clarification from the heads of departments within Sanlam Insurance company. Data collected by semi-structured interviews was recorded both on audio and written form after obtaining consent from the respondent.

Both the questionnaire and interview sought to collect data to explore the understanding from the practitioner perspective how the operational risks indicators are related to the claim processing operations and to determine how potential operational risks could be monitored using the identified operational indicators in an insurance firm case of Sanlam Insurance Company. Further, the respondents were expected to provide their perspectives on the extent to which technology has been or can be used to help in

monitoring the operational risks through the operational risk indicators in the claim processing leading to mitigation of the occurrence of the potential risks. In light of the Covid-19 pandemic, containment and safety measures in place, the researcher was limited from physical conduct of the interview and therefore virtual mode of conducting of the interview was adopted.

3.7 Data Analysis

3.7.1 Data Cleaning

Since the data collected contained attributes that were not necessary for the development of the frameworks, data cleaning was done. Whereas the way operational risks manifest is dependent on the organisational contexts, the underlying risk management principles are similar (White, 2005). Therefore, the data was checked for correctness based on the existing risk management principles. Where there were missing responses, piece-wise deletion technique of handling missing data was applied to ensure a balanced data set was used in the study.

3.7.2 Data Grouping

To develop and test the predictive ability of the proposed framework, there was a need to categorise the predictive operational risk indicators of the operational risks in the claims processing. The operational risk indicators were grouped based on Tripp (2004 proposition as cause-related, loss related and exposure related indicators. Both explanatory (descriptive) and exploratory analyses were conducted. Specifically, explanatory analysis quantitatively described the core attributes of a dataset that were relevant to the study.

3.7.3 Descriptive and Inferential Data Analysis

As indicated in section 3.3, the study adopted a mixed research strategy. Thus the qualitative and quantitative research approaches were adopted. The qualitative research method helped to gain insights into the problem of monitoring operational risks in the claim processing operations at Sanlam Insurance Company by examining the opinions of specific participants (Fletcher, 2017)[1]. It also provided a means of gaining deeper understanding of the opinions behind the given phenomena by answering the research questions: what are the claim processing operations in an insurance firm? The qualitative research methodology would also help answer some aspects of the research

question: How has information communication technology been utilised to monitor operational risks at Sanlam Insurance?

Descriptive analysis was conducted to determine what are the operational risks associated with the claims processing and approaches of monitoring them at Sanlam Insurance and the type of information communication technology utilised to monitor operational risks at Sanlam Insurance. The frequency, percentages and averages were the main descriptive statistical measures used for determining the existence of the operational risks indicators at the company under study and establishing the technology adoption in the company.

To obtain descriptive statistics from qualitative data, it was converted into quantitative formats by first identifying the themes based on the study constructs/variables and then creating codes based on the themes. Since, different insurance companies have configured product and service delivery based on the organisation structure, there was a need to conduct descriptive data analysis to determine the kind of operational risks associated with the claims processing at Sanlam Insurance.

Inferential analysis was conducted to determine the relationship between the claim processing operations and the existing operational risk indicators. The inferential statistical analysis was conducted based on the quantitative data collected using the questionnaires.

3.8 Proposed Framework Development structure

The proposed framework was developed on the basis of existing knowledge on operational risk management procedures in the claims processing operations in the insurance firm. The framework provides an immutable distributable database built on the Ethereum public Blockchain architecture. The Blockchain contains the ledgers that records all activities that occur in the claim processing operations. The main elements or data collection points used to build the ledgers of the Blockchain include the claim processing operations, the key risk indicators and the type of operational risks in the insurance company. Therefore, the framework developed was influenced by the inter-connections made between the state variables such as inputs, outputs and internal factors (claims processing procedures). There were minimal assumptions about the physical behaviours of the framework components as they were considered of less importance to

the proposed research. The type of operational risks likely to occur in the company will be dependent on the summation results of the kind of operational risk indicators flagged out based on the claim process operations. All these activities are recorded in the Blockchain for future auditing and reporting. This structure of the framework is data-driven owing to the attribution of data in the implementation process.

Through the Ethereum Blockchain network architecture, the proposed framework is developed such that external, and internal validators or nodes provide a peer for transaction endorsement and block commitment. Since the study did not aim at changing institutional structures as far as claims processing is concerned but rather explore ways in which Blockchain Technology could be used to enhance monitoring operational risk. The design of the proposed framework was therefore modelled on the integration of the technology on the existing claim processing procedures. Therefore, the design of the proposed framework was conducted by considering the general claims activities flow and the associated operational risk indicators.

The operational structure of the proposed framework is based on the following:

Client application – all client claim request proposals are to be stored on the Blockchain network which can be accessed by the internal validator

When the internal validator makes a request to view client claim requests this will be logged and the claims manager will receive the request and validate it as per client and this will then form a block of requests. The claims manager would therefore have control over access to information and any breaches/invalid requests can be monitored.

At reporting periods, the proposed framework would generate operational loss data for the period as a flag. Once the internal validator passes it to moves to the next level, it adds it as a data element onto the block. This can then be utilised by the management to intervene through requiring extra information for breaching thresholds, thus triggering further actions.

3.9 Research Quality

3.9.1 Reliability

Reliability of a research instrument relates to the consistency of a measure and concerns the extent to which the instrument yields the same results on repeated trials (Heale & Twycross, 2015). The reliability test of the study instruments was enhanced through conducting a pilot study using a pilot sample representative of the target population. This test was expected to refine the interview schedule (see appendix 2) so as to reduce response error rate by the respondents. According to Cooper and Schindler (2014), a pilot test with 10% to 30% of the sample respondents is adequate for examining the quality of the research instruments.

The pilot study was conducted with 10% of the sample respondents. The reliability of the interview schedule will be tested using an internal consistency method based on the Cronbach Alpha. According to Sekaran and Bougie (2013) Cronbach Alpha coefficient values ranges between 0 to 1 and the higher its coefficient the more reliable a research instrument is while purporting that reliability scores greater than or equal to 0.7 is a standard measure of asserting that the data collection instruments can be used for the research. From the pilot study, the Cronbach Alpha coefficient obtained was 0.72 which implied the instrument was reliable for the data collection.

3.9.2 Validity

Validity of a research instrument is the degree to which results obtained from the analysis of the data actually represent the phenomenon under investigation (Orodho, 2008). Additionally, validity of a study can be divided into two, namely: internal and external. Internal validity is explained as the study being able to achieve what it set out to achieve while external validity is defined as the degree to which the results of a study can be generalised to other people, situations and times (Saunders et. al, 2016). External validity establishes whether the content in the interview schedule measures the research variables accurately and effectively.

The research employed construct and content validity. Content validity looks at whether the instrument adequately covers all the content that it should with respect to the variables while construct validity refers to whether inferences can be drawn about test scores related to the concept being studied (Heale & Twycross, 2015). To ensure content validity the study incorporated face validity via zoom call with the supervisor subjecting the interview schedule to intensive expert review in order to make adjustments and/or additions to the research instruments as necessary. Confirming that all aspects of the

research variables are covered in the interview schedule in order to yield consistent results, the construct validity was tested.

3.10 Ethical Considerations

The requisite ethical considerations were observed by the researcher during this study in order to maintain research quality. The researcher applied for a research introductory letter from Strathmore University which was used to seek a research permit from the National Commission for Science, Technology and Innovation (NACOSTI) prior to the data collection process. The researcher further took guard of the identity of the respondents by ensuring that anonymity of the respondents was maintained in the course of the study. The researcher also ensured that all the collected data was used only for academic purposes and confidentiality was maintained in the study process.

The researcher sought for consent of the respondents to undertake the exercise. Further, the respondents were made aware of their rights relating to their participation in the study. This will be done in order to conform to the principle of voluntary consent by letting respondents willingly participate in the research (Saunders ,, 2016). Finally, the researcher respected the intellectual property rights by avoiding plagiarism (Kothari, 2011). That means that all materials which were used or referred to in this study were acknowledged accordingly and cited properly.

CHAPTER FOUR

RESEARCH FINDINGS

4.1 Introduction

This study sought to develop a framework for monitoring operational risks involved in claims processing using Blockchain Technology with a focus on a local subsidiary of an international insurer due to its infrastructure and capacity to implement such complex technology. The objectives of the study were to determine the operational risks associated with the claims processing in an insurance firm in Kenya, to determine the indicators of operational risks in claims processing in an insurance firm, to review on how information communication technology has been utilised to monitor operational risks in insurance and to propose a framework for monitoring operational risks that uses Blockchain Technology.

4.2 Demographic Characteristics of the Respondents and the Insurance Company

This section presents the results of the characteristics about the respondents and the insurance company considered in this study.

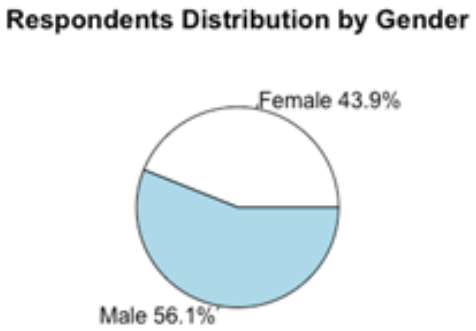
4.2.1 Response Rate

The response rate from the target population was recorded at 100%. This was partly attributable to the size of the population which was small, the great interest and motivation of the participating respondents in the research area that was responding directly to their current challenges and the nature of the tools used in data collection and administration approach which took into consideration the working condition and time of the respondents. The result further demonstrated a good response rate was obtained hence data was considered adequate for the study and it surpassed the threshold of 50% as stated by Bryman and Bell (2013) for this kind of study.

4.2.2 Respondents by Gender

The findings showed that the majority of those that responded were male respondents at 89%. This implies that there are few female heads of departments/officers in the insurance company. Figure 4.1 shows the distribution of the respondents by gender.

Figure 4. 1: Gender of Respondents

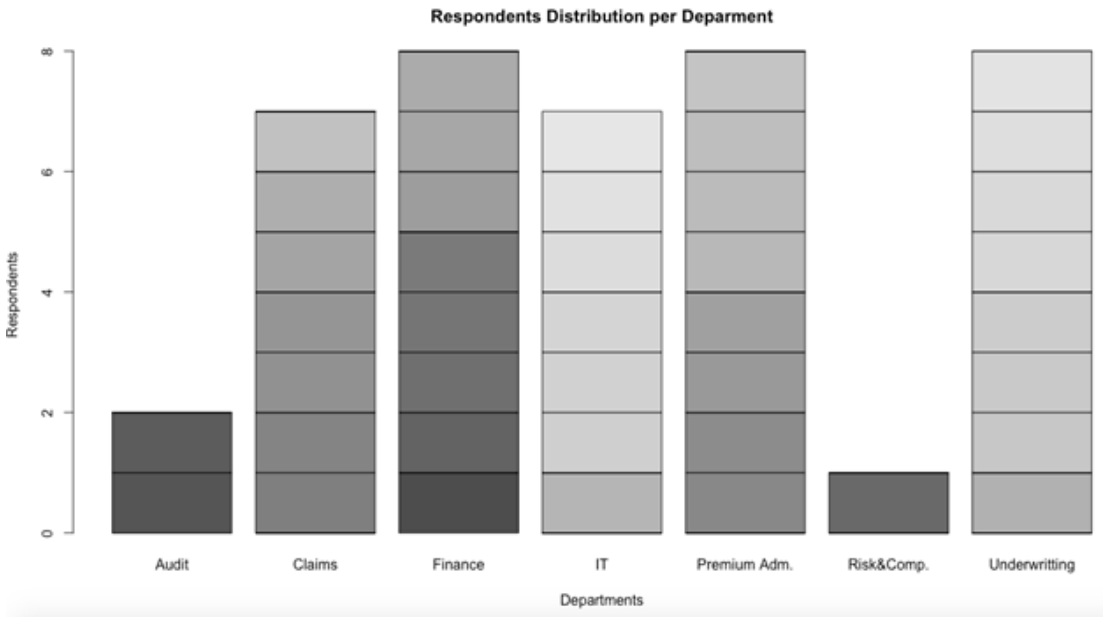


Source: Emma I Maraga (2022)

4.2.3 Distribution of respondents per Department

The key departments in Sanlam Insurance company involved in the claims processing includes claims, Internal audit, finance, Premium administration, IT and Risk & Compliance departments. The percentage distribution of the respondents from these departments was as follows; Claims 22%, Risk & Compliance 22%, IT 22%, Internal Audit 11%, Finance 11%, and Premium Administration 11%. This is presented in Figure 4.2.

Figure 4. 2: Department of Respondents

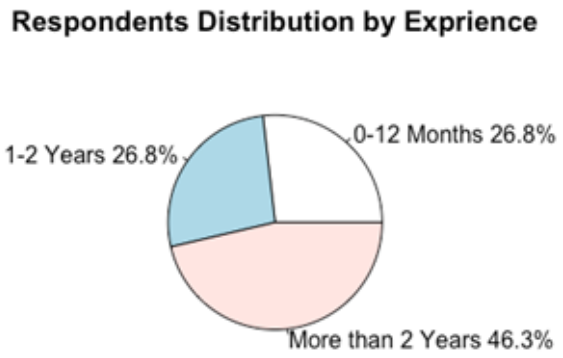


Source: Emma I Maraga (2022)

4.2.5 Work Experience of Respondents

The study sought to find out the work experience level of the respondents in the organisation. According to the findings presented in Figure 4.4 majority of the respondents, 56% had 2 or more years of work experience while 22% of the respondents had between 0-12 months and 1-2 years of work experience. This indicates a low staff turnover rate for the company.

Figure 4. 4: Work Experience of Respondents



Source: Emma I Maraga (2022)

4.3 Descriptive Analysis of Study Variables

This section describes the analysis of the study variables. The discussion focuses on operational risk indicators at Sanlam insurance company, operational risks associated with claims processing, information communication technology utilisation in monitoring operational risks and application of Blockchain technology framework for monitoring operational risks in the claims processing in insurance. To objectively measure the contribution of the operational indicators on the actual operational risks, an aggregated index score was developed. The relationship below was used to compute the index score.

$$Operational\ risk\ Index\ score = \frac{(Number\ of\ risk\ indicators\ \times\ \%\ value\ of\ indicator)}{rank}$$

Where the rank represents the position of the indicators when ranked based on the frequency score of the indicators, % value of indicator is determined from the number of respondents that gave high ranking on any one particular measure; and number of

indicators relates to the exact number of indicators considered per each section of the interview schedule.

4.3.1 Indicators of Operational risks in claims processing in an insurance firm

As pointed out in section 2.3.1, operational risk indicators are an important tool within operational risk management and understanding them contextually is key in overall management of the potential risks. It is argued that operational risks are dependent among other factors on the organisational structure, policies and governance structures (Deloitte & Touche (2020). It can therefore be inferred that the influence of particular indicators in one organisation might not necessarily lead to the same outcome on another. The study therefore sought to determine the influence of different categories of operational risks on the claim processing in the insurance firm focused by this study. The operational risk indicators considered in this study were grouped into cause-related indicators, loss-related indicators and exposure related indicators based on Tripp (2004) proposition.

4.3.1.1 Exposure Related Indicators Descriptive Statistics

Exposure related risks are volume-based indicators that allow measurement throughout processes likely to incur operational failure. The findings from the study presented in Table 4.1 shows that exposure related indicators which included; customer dissatisfaction, customer complaints and staff turnover are critical. 75.6% of the respondents identified customer complaints as the most likely exposure related indicators that could indicate the likelihood of existence of operational risks in a company. 65.9% of the respondents indicated that staff turnover was least likely to be a good indicator of the existence of operational risk in the insurance company. Partly this could be due to other factors not necessarily related to the operations at the company. The index scores were 1.51 and 0.34 respectively for both indicators.

Table 4. 1: Exposure related indicators likely to indicate existence/occurrence of operational risk

Exposure Related Indicators			
	Agree	**Disagree**	**Index Score of agreeing**
Client Complaints	75.6%	24.4%	1.51
Staff turnover	34.1%	65.9%	0.34

Source: Emma I Maraga (2022)

4.3.1.2 Loss Related Indicators Descriptive Statistics

Loss related indicators measure events associated with operational losses and are considered lagging indicators hence insufficient alone. The loss related indicators include errors, fraudulent activities, unauthorised activities, security breaches and misuse of data. From the findings shown in Table 4.2, all respondents identified errors and security breaches to be the most likely risk indicators that could imply potential existence of operational risks at the insurance company. Unauthorised activities were the least likely indicators of the occurrence of operational risks. This was also confirmed by the qualitative data with all the interviewers indicating that all employees have clearly defined roles & responsibilities with clear accountability lines. The index scores associated with each of the indicators are 5, 0.94, 0.15, 5, and 0.43 respectively.

Table 4. 2: Loss related indicators likely to indicate existence/occurrence of operational risk

Loss Related Indicators			
	Agree	**Disagree**	**Index Score of agreeing**
Errors	100%	0%	5
Fraudulent activities	56.1%	43.9%	0.94
Unauthorised activities	14.6%	85.4%	0.15
Security breaches	100%	0%	5
Misuse of data	34.1%	65.9%	0.43

Source: Emma I Maraga (2022)

4.3.1.3 Cause Related Indicators Descriptive Statistics

Cause related indicators measure factors identified as drivers for operational losses and are leading indicators. The factors considered in this study include IT failure and regulatory changes. From the findings presented in Table 4.3, 90.2% of the respondents indicated that IT failure will lead to operational risk in the company. This was collaborated with the data collected through interviews which identified IT systems to be critical in the operations within the claim processing division of the Sanlam Company. Regulatory changes was considered to be more external and thus not having direct implication on the operations of the company and hence could not most likely indicate the likelihood of occurrence of an operational risk. Moreover, from the interview, it was noted that the insurance regulatory framework in the country is fairly

developed and aimed at mitigating operational risks. Nevertheless, 24.4% of the respondents agreed that they could most likely infer the occurrence of operational risks in the company. Index score is 2.71 and 0.37 respectively.

Table 4. 3: Cause related indicators likely to indicate existence/occurrence of operational risk

Cause Related Indicators			
	Agree	**Disagree**	**Index Score**
IT failure	90.2%	9.8%	2.71
Regulatory changes	24.4%	75.6%	0.37

Source: Emma I Maraga (2022)

4.3.2 Operational Risks in Claims Processing

In section 1.1.2 it is pointed out that operational risks in the insurance industry have become more interconnected with increasingly complex interactions and many companies are collapsing due to poor operational management strategies (Insurance Regulatory Authority, 2017). Using the operational risk indicators investigated in section 4.3.1, the study sought to identify the operational risks associated with claims processing in an identifiable insurance company. According to Ohando (2015) some of the operational risks may include events and actions or inactions, such as fraud, human error, accounting errors and system failures. Based on the identified risk indicators in the claim processing at Sanlam, the respondents were asked to relate the indicators to potential operational risks that can occur in the claim processing. From the study 100% of the respondents identified human and accounting errors as the likely operational risks that can occur in the claim processing operations. This was confirmed by the respondents from the heads of department who indicated that in the recent past the cases reported in the company were attributable to human and accounting errors. 90.2% of the respondents also identified IT systems failure as the potentially high operational risk that can occur in the company. This could be explained by the fact that the company has adopted IT in its core operations and therefore an IT failure could have serious implications on the operations of the company. All respondents indicated that statutory reporting failure didn't appear to be a significant operational risk to the company. Table 4.4 shows the response on the identified possible operational risks in the claims processing.

Table 4. 4: Operational risks likely to occur in claims processing given the identified operational risk indicators in the insurance company

Operational Risks		
	% of respondents who agreed	% of respondents who disagreed
Fraud	43.9%	56.1%
Human errors	100%	0%
Accounting errors	100%	0%
System failure	90.2%	9.8%
Statutory reporting failure	34.1%	65.9%

Source: Emma I Maraga (2022)

The findings are consistent with the understanding that operational risks generally are as a result of operational events such as inadequacy or failure of internal systems, personnel, procedures, or controls, as well as external events (International Association of Insurance Supervisors, 2020).

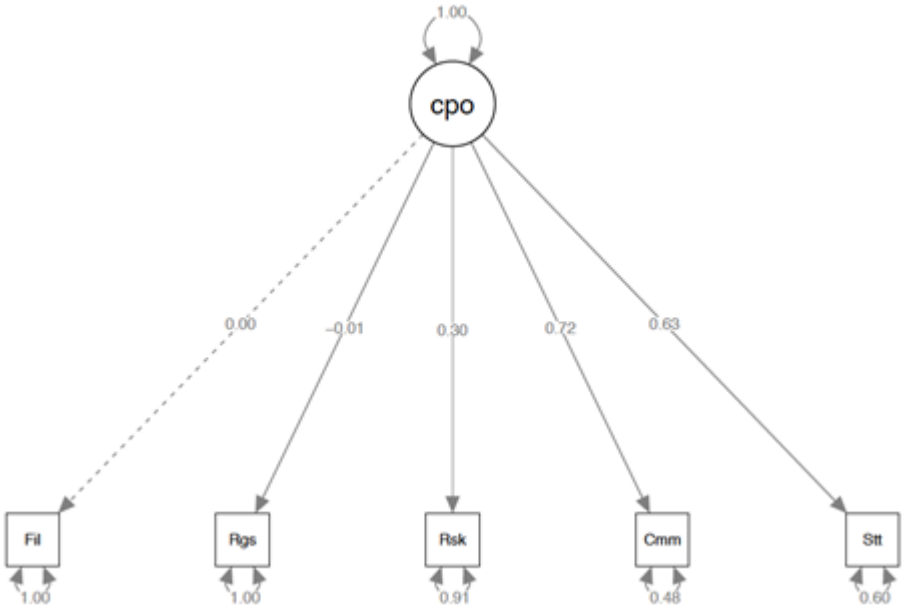
4.4 Information Communication Technology Utilisation in Monitoring Operational Risks

The respondents were requested to indicate whether their respective departments have adopted Information Communication Technology in the insurance organisation. 100% of the respondents indicated they have adopted ICT in the claims processing and they use ICT to complement their risk monitoring. They however indicated an adoption of Blockchain technology would be more effective in monitoring and flagging out the risks by tracking the risk indicators. In terms of the specific attributes of the Blockchain they would prefer, immutability and finality characteristics of the Blockchain were considered important by all respondents at 100%. The other attributes of the Blockchain were considered not important to the company at an average of 73.2% for consensus and 100% for the provenance.

4.5 Link between Operational Indicators and Types of Operational Risks

To determine if the identified operational indicators could be used to determine the type of operational risk at Sanlam, the structural equation modelling technique was used. The first step was to determine the loading levels of the various operational process's factors at Sanlam company. Figure 4.3.1 gives the factor loading of the operational processes that collectively define the claims processing at Sanlam Company.

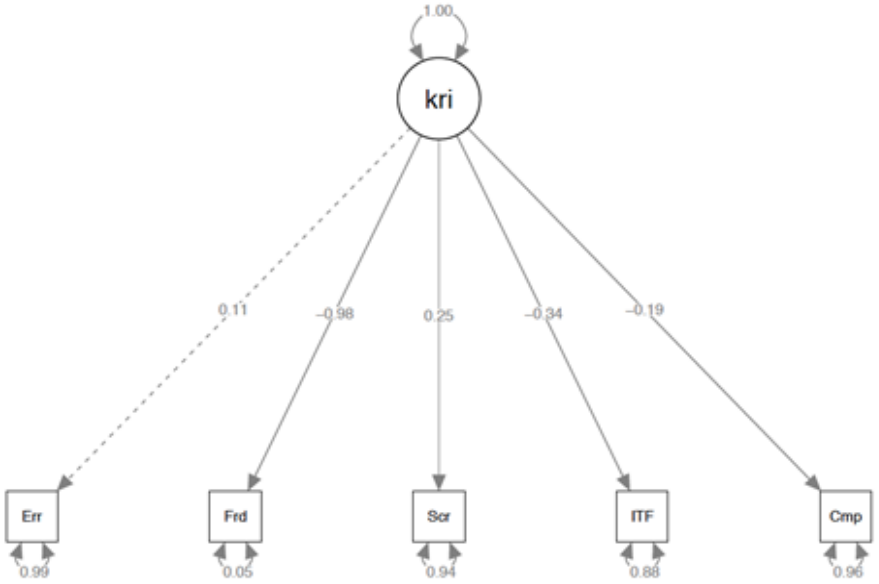
Figure 4.3.1: Factor loading for Sanlam claim processing Operations



From 4.3.1, communication and claim settlement was considered critical. And since this is a service industry, the client experience will be enhanced by these two operations.

The second analysis involved the determination of the loading factors for the key risk indicators at Sanlam. Since data misuse and unauthorised risk activities were considered by the respondents as not important as detailed in section 4.3.1.2, they were not included in this analysis. Figure 4.3.2 shows the outcome of the analysis:

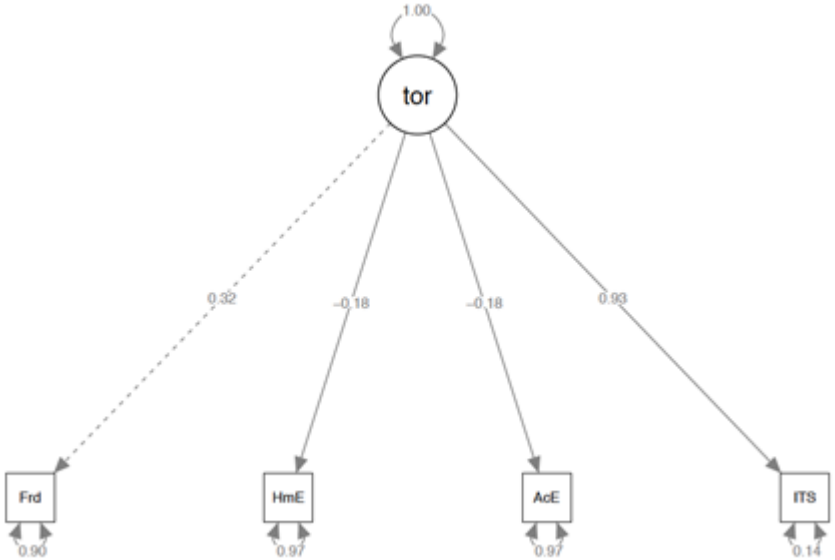
Figure 4.3.2: Risk Indicators loading at Sanlam Insurance Company



It was established that all the identified indicators retained were loading into the collective measure of the risk indicators with the Error indicator loading significantly.

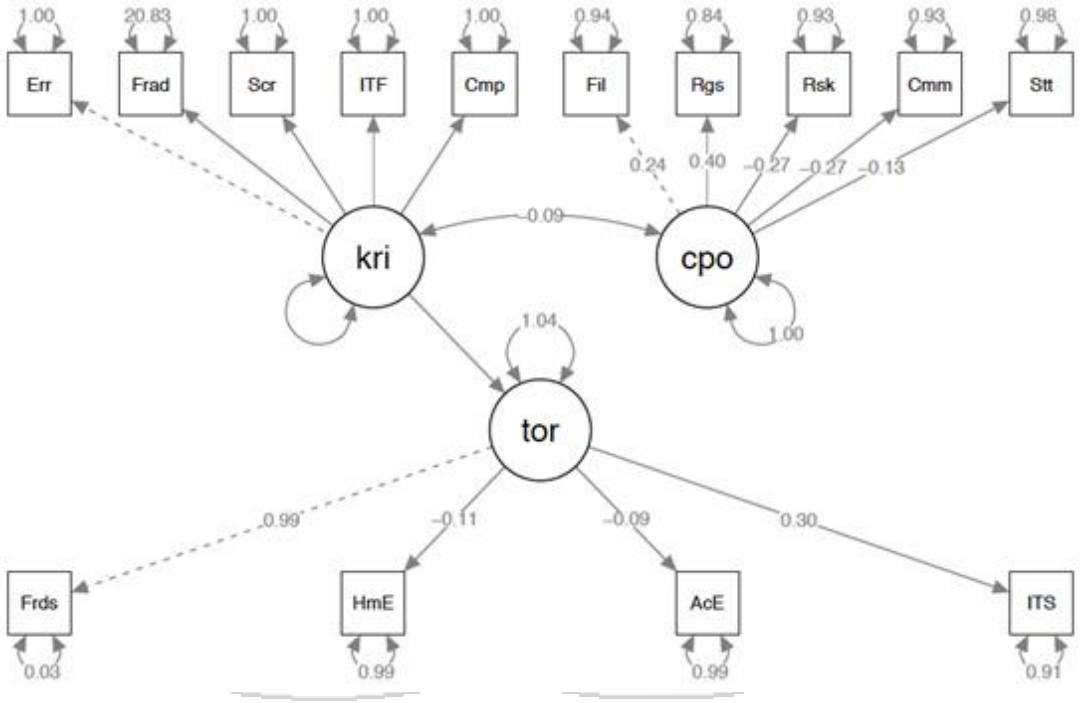
An analysis was also conducted to determine if the identified type of operational indicators at Sanlam were loading collectively. Figure 4.3.3 shows the outcome of the analysis with IT systems failure loading significantly followed by Fraud.

Figure 4.3.3: Factor loading for type of operational risks at Sanlam Insurance Company



After establishing the factor loading, analysis to determine the structural relationship between the measured variables, that is, the company operational processes (CPO), the key risk operational indicators (KRI) and the type of operational risk (TOR) at Sanlam insurance company. Figure 4.3.4 shows the structural relationships analysis as identified by the conceptual model in section 2.9.

Figure 4.3.4: Structural analysis of the relationship between CPO, KRI & TOR at Sanlam Insurance Company



From figure 4.3.3, it demonstrates that there is a covariance relationship between a company's operational processes (CPO) and the key risk indicators (KRI). This means the two and could be used to determine the type of insurance risks at Sanlam. When the COP and KRI are considered, the factor loading for the tor changes significantly with fraud loading highly at 0.99 followed by ITS at 0.30. This effectively means that to determine the type of operational risk at Sanlam one will need to know the operational processes and the risk indicators used to measure them. This forms the foundation upon which a model to monitor the claims processing risk at Sanlam could be built.

Armstrong and Preston (2019) indicate that to effectively manage the operational risks, there is a need to monitor them. The structural model in figure 4.3.3 demonstrates the link or relationship between the indicators and the operational risks at Sanlam.

4.6 Proposed Framework for Monitoring Operational Risks using Blockchain Technology in Claims Processing in Insurance

In section 4.3.1 the risk indicators that should be understood in order to flag out potential operational risk have been established. Further in section 4.4, a link between the risk indicators and the possible operational indicators in the claims processing has been determined.

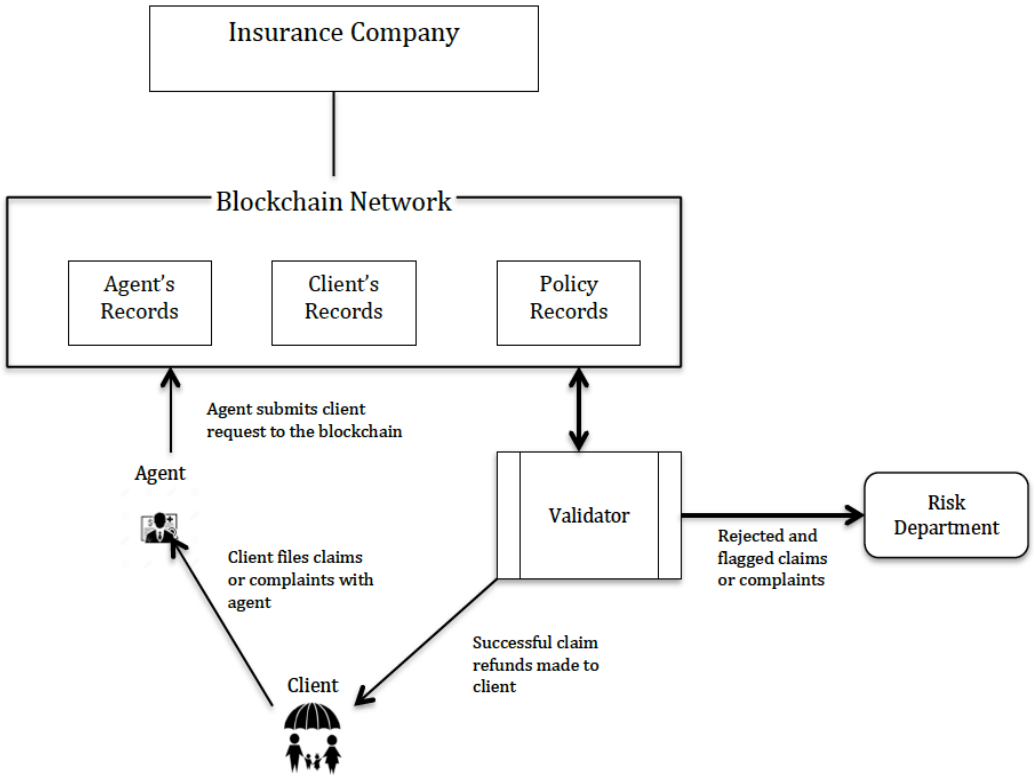
The proposed framework is built by taking into consideration the conceptual framework and the study findings which confirmed that the operational risks based on the existing claims processing operations are important in monitoring potential operational risks in the Sanlam Insurance company. Since the identified operational risks are largely attributable to human intervention, we propose the use of Blockchain Technology which provides a secure means of securing the records from alterations. In the event there are alterations the Blockchain provides the footprints of the changes which can be used to monitor the changes through its immutable and finality characteristics which the respondents considered important for their company.

Based on these findings, the proposed framework is modelled on the claim processing flow. It takes into consideration the following key claims processing stages: filing of notification by the client to insurer including all necessary documentation attached through the insurance agent; policy checks and reviews used to check for validity by the validators using predetermined evaluation/assessment criteria; and lastly, settlement of the claims through payment.

At each stage of the claim processing the framework proposes the building of an immutable block of records that build into a Blockchain network as indicated by the respondents in section 4.5. Further, at each given stage of the process, there can arise various operational risks as identifiable through the encoded or in-built risk indicators. Since, the records in the Blockchain are immutable and developed based on predetermined agreements, the potential deviations or would be added onto the original record without changing it. This is flagged out at the validation stage and reported to the relevant department.

The proposed framework utilising Blockchain Technology can provide clients and insurance companies with the means of managing claims in a transparent, irrefutable and responsive manner. The framework allows for filing claims records onto a Blockchain-facilitated data repository. The claims are then validated using advanced analytics and real-time data sources by the network. The validators will be built based on the claims processing policies and procedures of an insurance company. In the claims processing, the policies are formulated from the indicators of the operational risks. The operational risk indicators are used to flag out potential challenges associated with a specific claim and hence be reported to the risk department for further action. The Blockchain rejects a claim which fails to meet the set criteria inbuilt in the validator. Figure 4.5 shows a proposed framework for monitoring operational risks in the claims processing.

Figure 4. 5: Framework for monitoring Operational Risks in claims processing



CHAPTER FIVE

5. DISCUSSION, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter focuses on discussing the study findings; the conclusion based on the study objectives; the recommendations drawn from the study outcomes and proposes possible areas for further studies.

5.2 Discussion of the Research Findings

5.2.1 Operational Risks associated with Claims Processing in an Insurance firm

The study findings established that human and accounting errors at 100% were the prevalent operational risks associated with the claims processing at Sanlam Insurance company. IT systems Failure at 90.8% was identified also as the most likely operational risk at Sanlam. Other operational risks are fraud at 43.9% and statutory reporting failure at 34.1%. These findings are consistent with the findings of study by Hirsh and Cha (2015) and Hunter (2011) who argue that since human errors can occur at different levels through data entry errors, procedural errors, among many other errors that can be made they largely present the most common and most significant risk to any organisation or individual. Similarly, it may also indicate a lack of skilled staff able to effectively and diligently input data evolving from human error.

5.2.2 Indicators of Operational Risks in Claims Processing in an Insurance firm

Operational risk indicators of the insurance organisation were categorised into; exposure related indicators, loss related indicators and cause related indicators. Concerning exposure related risk indicators, the study findings showed that the most prevalent exposure related risk indicator is client complaints as indicated by an index score of 1.56 with 75.6% of the respondents identifying it as a good indicator of potential risk. This finding supports Tripp (2004) thoughts that customer dissatisfaction or complaint is an indicator that gives the insurance company the external impact of any failure within the claims process. Grove (2011) further points out that, if time is not kept (TAT - Turnaround Times) or benefit has not been calculated correctly and there

appears to be a decline in the claims process, the most appropriate response/feedback comes from the affected customers in terms of dissatisfaction.

Loss related risk indicators, findings from the study showed that errors and security breaches with index scores of 5 are the most prevalent indicators that can point out potential operational risks. This finding is consistent with the findings by Hirsh and Cha (2015) that state that the claims process involves assessment which is subject to some level of human intervention and errors can occur through data entry errors, procedural errors, among many other errors that can be made. Hunter (2011) further points out that errors are the most common and most significant risk to any organisation or individual. Similarly, it may also indicate a lack of skilled staff able to effectively and diligently input data evolving from human error. Consequences of incorrect input may be multiple, including incomplete information, incomplete understanding, insufficient knowledge, inconsistent processing, genuine input error, or more. Majority of the interviewee's agreed that severity and impact of human error can be catastrophic to the insurer, either through operational losses, financial loss, reputational damage, and incur regulatory or legal fines and penalties.

Cause related risk indicators showed that IT failure is the most prevalent cause related indicator with an index score of 2.71. Further the findings consider regulatory changes at index scores of 0.34 to also infer potential operational risks. This finding is supported by the study by Sheehan (2020) who states that most insurers suffer from loss in policyholder numbers during recessions. This can be attributed to policyholders choosing to lapse, cancel, withdraw, and surrender their insurance policy in favour of retaining that income to sustain themselves during the economic downturn. In the recent past, a report by Deloitte & Touche (2020) on insurance outlook argues that despite the efforts put in place by governments to cushion the public from the adverse economic effects, the Covid-19 pandemic will likely result in long-term impacts, slow recovery, and uncertainty as the insurance industry take time to recover.

Conclusions made indicate that monitoring of operational risks in claims processing can be done by identifying areas that need to be adapted or changed. This enables identification of trends and patterns, adoption of strategies and informing decisions made on actions to be taken. Process monitoring tracks the use of inputs and resources, the progress of activities, and the delivery of outputs.

5.2.3 Information Communication Technology Utilisation in Monitoring Operational Risks in Insurance

The study sought to review how information communication technology has been utilised to monitor operational risks in the insurance organisation. 100% of respondents agreed that the insurer has adopted ICT especially within the claims department. The study also found out that despite adoption of ICT, there were differences in respondent views on extent of adoption. Majority of respondents agreed that the claims process is automated however there are still manual workarounds within the process which contribute to operational risks.

Respondents were also asked to describe the role IT plays in operational risk management and replies included; report generation that is used to assess and monitor operational risks, workflows within the claim process to track human errors especially within archiving systems, articulation of needs by departments and IT develops solutions, automated calculation of benefits and claims, segregation of duties, and integration with bank platforms for seamless payments, embedded controls within the process, automated approval matrix embedded in the claim amount processing, process and risk review checklists, incident management, and complaints tracking.

In concurrence with these findings, Stein (2006) points out that several claims processing technology vendors exist in the market today offering a range of services that allow for recording of claims, ability to approve and validate, escalation to senior management, AML screening of clients, and integration to other systems in the claims processing cycle. This integration includes links to banks, assessors, adjusters, medical and smart card providers, and mobile money services. The current focus of claims processing technology is ensuring a system that offers speedy assessment whilst maintaining robust service delivery. Neale (2020) further supports the above study by stating that for insurers to survive long-term, their ability to innovate is important, with majority of insurers today focusing on automating and improving the claims process. Current improvements involve telematics, augmented reality, drones, and other remote inspection technologies as discussed in chapter 2.

Sheehan (2020) states that use of gamification in the insurance industry is gaining rapid traction and is considered as a powerful tool to spur massive growth within areas of historically low performance. The author additionally states that though gamification is not a new technology, many insurers have recently started to adopt it as a way of

creating more customer-centric digital solutions. Due to its relatively low implementation cost, gamification is currently one of the prevailing IT trends in insurance. Grove (2011) further supports these findings by pointing out that operational risks related to employment practices and workplace safety can then be monitored through gamified elements. Additionally, risk associated with employee relations, diversity, and inclusion in the workplace can be monitored and addressed through incentives for employees to produce, learn, and become more resourceful.

As more and more insurers adopt automated claims processes, this will effectively eliminate some operational risks related to human error as no manual interventions will be needed but still retain system related operational risks. Due to the complexity, data requirements, and system capability required for the insurer to begin implementation of Blockchain Technology; they are likely to begin moving towards that direction by first adopting the simplest and least costly solutions and progressively increasing complexity until full Blockchain implementation.

5.2.4 Application of Blockchain Technology for Monitoring Operational Risks in Claims Processing in Insurance

The study considered the level of importance of Blockchain characteristics attached by the various departments at Sanlam. The main characteristics considered included; consensus, provenance, immutability, and finality. Majority of respondents at 100% agreed that immutability and finality were the most important characteristics of Blockchain since they will ensure there is sufficient ownership of risk and the ability of the technology not to be manipulated in any way. Neale (2020) supports these study findings pointing out that Blockchain Technology has the capability to make monitoring operational risk easier and more accurate due to its *immutability* and capacity for large amounts of data. Likewise, there will also be a corresponding increase in security, decrease in fraud, increase in efficiency and record sharing as well as a decrease in costs associated with both the claims process and in monitoring operational risks. Sayegh (2018) states that Blockchain has the potential to eliminate inefficiencies from intermediaries, allow for programmable direct interaction with policyholders, permit use of smart contracts programmed to release payments or trigger alerts due to breaches of operational risk limits.

5.2.5 Framework for Monitoring Operational Risks that uses Blockchain Technology in Claims Processing in Insurance firms in Kenya

In order to fully embed and implement the proposed framework, insurance companies will need to give extra attention to the following components that are key in enabling the Blockchain network to work.

Client requests – all client claim requests are stored on the Blockchain network which can be accessed by the internal validators (claims, risk & compliance, finance, forensics, and audit departments) based on agreed format and standards.

When the internal validators make a request to view client claim requests this is logged and the claims department receives the request per client which is then logged on the network ledger once validated forming a block of requests. This would mean that the claims manager has control over who has access to information and how much information an individual can request access to. Any breaches/invalid requests can then be monitored and if found to be unauthorised, using the token system within Blockchain the claims manager can be rewarded or penalised.

Another internal peer is the finance department who provides audited financial operational loss data in real time to the risk and compliance department in order to carry out monitoring. The Blockchain network would be set up in a manner that triggers responses based on operational loss risk appetite breach as per set rules. If the risk appetite is breached, using smart contracts a notification is sent to the risk and audit department, finance (if trigger requires release of capital), and senior management.

At defined reporting periods, Blockchain can be set up to generate operational loss data, capital releases, and operational risk appetite breaches for the period. This can then be utilised by management to make strategic decisions or further probe operational risks and re-evaluate controls in place to manage their severity and impact. The network can also be set up in such a manner that operational loss data at the end of every quarter is sent to the regulator which can form part of their database and aid in their regulation of insurers.

As part of the validation checks, policy details were confirmed within the network and validated as well as premium attached to the policy which ensures policy status is active in event of claim request. This leads to a faster insurance payment process, end-to-end system automation for efficiency and reduction in errors.

The proposed framework is based on the metrics developed from the monitoring indicators and aligned to the company claims processing guidelines and procedures. As indicated by Shiller (2006) to construct reliable monitoring risks sometimes may call for referring to the identified risk exposures over time which will provide relevant data to develop a flagging function. It is therefore imperative that insurers should seek to monitor levels of operational risk exposure as a formal process and fundamental business requirement. This proposition is also supported by Finlay (2004) who argues that in forward-looking analysis of operational risk there will be a need to have sufficient key risk indicator monitoring data.

5.3 Conclusions

From the findings human errors and accounting errors are the most prevalent operational risks as identified by 100% of the respondents. Other operational risks identified include system failures at 90.2%%, fraud at 43.9%%, and statutory reporting failure at 34.1%. All respondents indicated that statutory reporting failure didn't appear to be a less likely operational risk to the company due to the existence of a well-established insurance regulatory framework in the country.

The main operational risk indicators based on the established category were found to be client complaints at 75.6% was prevalent for exposure related operational risk indicators, errors and security breaches at 100% loss related risk indicators, and IT failure at 90.2% for cause-related risk indicators. Further, at a covariance level of 0.09 it established the existence of a positive relationship between the operational risk indicators and the operational processes at Sanlam Insurance company. Which may imply objectivity in measuring the types of operational risks in the company.

From the findings, it was established that the adoption of ICT in the insurance company is well received at 100%. The immutability and finality characteristics of the Blockchain were considered more important with 100% of the respondents selecting them. Based on these findings, the researcher proposes a framework utilising Blockchain Technology that can provide clients and insurance companies with the means of managing claims in a transparent, irrefutable and responsive manner by using the immutable characteristics of the Blockchain Technology. The framework provides a secure means of submitting claims by the client through the respective agents who do

not have any ability to alter the submitted records from the clients. The claims are then stored in a secure repository that is accessible by authorised users without any room for altering the records. The users can however be allowed to add into a record without altering its original formats or values. Whereas any attempt to alter the record may not be successful, it can however be recorded and flagged out at the validation stage based on the predetermined criteria.

5.4 Recommendations

The recommendations based on the findings and conclusions of the study were made in two parts. They include recommendations for improvements and recommendations for future research.

5.4.1 Information Communication Technology Utilisation in Monitoring Operational Risks

5.4.1.1 Operational Risks associated with Claims Processing

The study established that there exists a statistically significant positive correlation between operational risk indicators (fraudulent activities, staff turnover, security breaches, IT failure, complaints) and operational risk flags (fraud, human errors, accounting errors, system failure, statutory reporting failure). The study recommends that for an effective Blockchain operational risk monitoring process, extensive data collection on operational losses both with respect to severity and impact is required for effective quantification of operational risk indicators and monitoring of operational risk. Additionally, having a comprehensive set of risk indicators along with corresponding escalation triggers will enable an effective risk reporting process. This may entail having a good database of losses on operational failure, quantitative targets for improvement and good techniques for predictive analysis.

5.4.1.2 Information Communication Technology Utilisation in Monitoring Operational Risks

The study established that insurers are seeking to implement modern claims systems or enhance their existing claims systems, leverage advanced fraud detection technologies, and innovate around self-service and straight through processing. The study recommends that organisations looking to be successful in an environment of uncertainty should give emphasis on innovation particularly Blockchain Technology,

increased risk tolerance and striving for a culture of change acceptance and adaptation in order to thrive in the insurance industry.

5.4.1.3 Application of Blockchain Technology for Monitoring Operational Risks in Claims Processing in Insurance

The study established that Blockchain Technology has the capability to make monitoring operational risk easier and more accurately due to its immutability attributes. The study therefore recommends that insurance companies should incorporate Blockchain Technology to reliably monitor possible operational risks through the approved operational risk indicators. It further recommends that within the claim process, smart contracts can be deployed throughout to notify, assess, or pay claims and collect data.

5.4.2 Recommendations for Future Research

Whereas the study was limited to a case study focusing on a single company, future research could be done to; further validate the proposed framework, to confirm the performance of the framework under different contexts, and to test the framework against other existing frameworks if available.

REFERENCES

Abbas D., Ismail T., Taqi M., and Yazid H. (2021). Determinants of enterprise risk management disclosures: Evidence from insurance industry. Accounting 7 (2021) 1331–1338. https://doi:10.5267/j.ac.2021.4.005

Acharyya, M. (2012). Why the current practice of operational risk management in insurance is fundamentally flawed - evidence from the field. ERM Symposium, April 18-20, 2012, p. 5

Adam, J. (2005). Managing Business Risk. 2nd Edition. GBR: Kogan Page Ltd.

Ajupov A., Sherstobitova A., Syrotiuk S. and Karataev A. (2019). The risk-management theory in modern economic conditions. E3S Web Conf., 110 (2019) 02040. https://doi.org/10.1051/e3sconf/201911002040

Akkizidis, L. S., & Bouchereau, V. (2005). Guide to Optimal Operational Risk and Basel II. New York: Auerbach Publications, Taylor & Francis Group.

Akkizidis I., & Khandelwal, S. K. (2008). Operational Risk in Islamic Finance. In: Financial Risk Management for Islamic Banking and Finance. Palgrave Macmillan Finance and Capital Markets Series. Palgrave Macmillan, London. https://doi.org/10.1057/9780230598751_6

Akomea-Frimpong, I., Andoh, C., & Ofusu-Hene, E. D. (2016). Causes, effects and deterrence of insurance fraud: Evidence from Ghana. Journal of Financial Crime, 23(4), 678-699.

Alexander, Kern. (2014). Stability and Sustainability in Banking Reform: Are Environmental Risks Missing in Basel III? 10.5167/uzh-103844.

Amorose, R. C. (2011). Driving operational excellence in claims management. USA: Deloitte Development.

Arnheiter, E. D., & Maleyeff, J. I. (2005). The Integration of Lean Management and Six Sigma. The TQM Magazine, 17(1), 5-18.

Arrow, K. J. (1971). Essays in the Theory of Risk Bearing, Markham, Chicago, IL.

Ashturkar, P. B. (2014). Comparative study of effectiveness of claims settlement operations in Indian life insurance companies. International Journal of Advance Research in Computer Science and Management Studies, 2(11), 148-155.

Asokere, A. S., & Nwankwo, S. I. (2010). Essential of insurance: A modern approach (1st edn.). Lagos: Fevas Publishing.

Association of Kenya Insurers (AKI). (2015). Insurance Industry Annual Report. Nairobi: Association of Kenya Insurers (AKI).

Association of Kenya Insurers (AKI). (2016). Insurance Industry Annual Report. Nairobi: Association of Kenya Insurers (AKI).

Association of Insurance and Risk Managers in Industry and Commerce (2009). Delivery excellence in insurance claims handling: Guide to best practice. London: AIRMIC.

Avolio, B. J., Yammarino, F. J., & Bass, B. M. (2009). Identifying common method variance with data collected from a single source: an unresolved sticky issue. Journal of Management, 17(3), 571-87.

Barros, R. H., & Torre-Enciso, M. I. M. (2012). Operational Losses for the Capital Charge of Health Insurers: Lessons from Spain. The Geneva Papers on Risk and Insurance. Issues and Practice, 37(4), 763–779. http://www.jstor.org/stable/41953208

Barros, R., & Torre-Enciso, M. (2013). Operational Losses for the Capital Charge of Health Insurers: Lessons from Spain. The Geneva Papers on Risk and Insurance. Issues and Practice, 37(4), 763-779. http://www.jstor.org/stable/41953208

Basel II Committee on Banking Supervision. (2006). Sound Practices for the Management and Supervision of Operational Risk. Available online at www.bis.org/publ/bcbs91.pdf.

Basel II Committee on Banking Supervision. (2004). Sound Practices for the Management and Supervision of Operational Risk. Available online at www.bis.org/publ/bcbs91.pdf

Baxter, P., & Jack, S. (2008). Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers. The Qualitative Report, 13(4), 544-559. https://doi.org/10.46743/2160-3715/2008.1573

Bendell, T. (2006). A review and comparison of six sigma and the lean organisations. The TQM Magazine, 18(3), 255-262. https://doi.org/10.1108/09544780610659989

Bendickson, J., Muldoon, J., Liguori, E. & Davis, P.E. (2016). Agency theory: The times are Changing. Management Decision, 54(1), 174-193. https://doi.org.ezproxy.library.strathmore.edu/10.1108/MD-02-2015-0058

Bernard, H. (2000) Social Research Methods: Qualitative and Quantitative Approaches, Sage, Thousand Oaks. https://www.scirp.org/(S(351jmbntvnsjt1aadkposzje))/reference/referencespapers.aspx?referenceid=1903641

Blunden, T., & Thirlwell, J. (2010). Mastering Operational Risk: A practical guide to understanding operational risk and how to manage it. 1st edition. Edinburgh: Pearson.

Bouriche N., Wilson G., Kishk M.(2021). An AHP- Structural Contingency Theory – Based Approach for Supplier Selection: Insights from an Algerian Industrialised Company. 4th ICBMF.

Breden, O. A. (2017). Integrated Risk Management Systems around the world. New York, Pearson Education.

Brennan, P. (2012). A comprehensive survey method for overcoming the class imbalance problem in fraud detection. A dissertation submitted for the Degree of MSc in computing of institute of Technology, Blanchard town. Dublin, Ireland.

Brooks, P. J., Popow, D. J., & Hoopes, D. L. (2005). Introduction to Claims. Pennsylvania: American Institute for Chartered Property Casualty Underwriters.

Capgemini (2011). Capturing operational efficiency and sustainable value through claims. Retrieved from http://www.capgemini.com/claims.

Chernobai, A., Jorion, P. & Yu, F. (2009). The determinants of operational risk in US financial institutions. Journal of Financial and Quantitative Analysis, 46(6), 1683-725 (Forthcoming – Proceedings of the 45th Annual Bank Structure and Competition Conference "financial regulatory reform", Federal Reserve Bank of Chicago).

Chernobai, A., Jorion, P., & Yu, F. (2011). The Determinants of Operational Risk in U.S. Financial Institutions. The Journal of Financial and Quantitative Analysis, 46(6), 1683–1725. http://www.jstor.org/stable/41409665

Chorafas, D. N. (2004). Operational Risk Control Business Opportunity and Challenges for the Insurance Industry. The Geneva Papers on Risk and Insurance. Issues and Practice, 29(1), 87–101. http://www.jstor.org/stable/41952747

Cochran, W. G. (2007). Sampling techniques. John Wiley & Sons.

Cooper, D. & Schindler, P. (2014). Business Research Methods. Mc-Graw Hill: New York.

Corbett, L. M. (2011). Lean Six Sigma: the contribution to business excellence. International Journal of Lean Six Sigma, 2(2), 118-131. https://doi.org/10.1108/20401461111135019

Corvellec, H. (2009). The Practice of Risk Management: Silence Is Not Absence. Risk Management, 11(3/4), 285-304. http://www.jstor.org/stable/40468443

Crawford, S. (2007). Trends in Claims Handling: Insurance Industry Update. Canada: Crawford & Company Inc.

Crocker, K. & Tennyson, S. (2002). Insurance fraud and optimal claims settlement strategies. Journal of Law and Economics, 45(2), 469-507.

Cummins, J. (1976). Risk Management and the Theory of the Firm. The Journal of Risk and Insurance, 43(4), 587-609. Doi: 10.2307/252028

Cummins, J.D., Wei, R. and Xie, X. (2012), "Financial sector integration and information spillovers: effects of operational risk events on US Banks and insurers", Working Paper, Temple University, Philadelphia.

Davis, J. H., Schoorman, F.D. & Donaldson, L. (1997). Toward a stewardship theory of management. Academy of Management Review, 22(1), pp. 20-47.

Dennis, W. (2005). Risk Management and Business Continuity, Overview, and Perspective. Prentice Hall.

Derrig, R. (2002). Insurance Fraud. Journal of Risk and Insurance, 69(3), 271-287.

De Vaus, D. (2006). Research Design in Social Research. London: SAGE.

Dexter, N. C., Ford, C. L., Jakhria, P. C., Kelliher, P. O. J., McCall, D., Mills, C. K., Probyn, A. C., Raddall, P. A., & Ryan, J. (2007). QUANTIFYING OPERATIONAL RISK IN LIFE INSURANCE COMPANIES: DEVELOPED BY THE LIFE OPERATIONAL RISK WORKING PARTY. British Actuarial Journal, 13(2), 257–357. http://www.jstor.org/stable/41141729

Dhanushkoti, S., & Coates, P. (2006). Insurance claims management - improving efficiency and effectiveness to reduce cost of claims. AIR Cover Story. Retrieved from: http://www.asiainsurancereview.com

Dickinson, G. (2001). Enterprise Risk Management: Its Origins and Conceptual Foundation. The Geneva Papers on Risk and Insurance. Issues and Practice, 26(3), 360-366. http://www.jstor.org/stable/41952578

Dionne, G. (2013), Risk Management: History, Definition, and Critique. Risk Management and Insurance Review, 16: 147-166. https://doi.org.ezproxy.library.strathmore.edu/10.1111/rmir.12016

DiNapoli, T. P. (2013). Improving the effectiveness of your claims auditing process. Office of the New York State comptroller. Retrieved from http://.www.osc.state.ny.us

Donaldson, L. (2001). The contingency theory of organisations. Thousand oaks, CA: Sage

Dorfman, M. S. (2007). Introduction to Risk Management and Insurance. The Chartered Insurance Institute of London.

Dowd, V. (2003). Measurement of Operational Risk: The Basel approach. Operational Risk. Regulation, Analysis and Management. Edited by Alexander, C. Pearson Education Ltd. Harlow.

Drennan, Lynn T. & McConnell, Allan (2007). Risk and Crisis Management in the Public Sector. Routledge.

Eckert, C. and Gatzert, N. (2019), "The impact of spillover effects from operational risk events: a model from a portfolio perspective", Journal of Risk Finance, Vol. 20 No. 2, pp. 176-200. https://doi.org.ezproxy.library.strathmore.edu/10.1108/JRF-09-2018-0143

Edward, W. C. (2001). Claim manuals and training materials: How to address them during discovery and trial. Dallas: Quilling Sellander Lownds Winslett.

Eisenhardt, K. M. (1989). Agency theory: an assessment and review. Academy of Management Review, 14(1), 57-74.

Esri, H. (2012). GIS for the Insurance Claims Process: Five Steps for an Effective Workflow. California: Esri Whitepaper.

Finlay, M. (2004). KRIs: An Industry Framework. Operational risk, July

Fletcher, A.J. (2017). Applying critical realism in qualitative research: Methodology meets method. International Journal of Social Research Methodology, **20**(2), pp. 181–194.

Flynn, B. B., Huo, B., & Zhao, X. (2010). The impact of supply chain integration on performance: A contingency and configuration approach. Journal of Operations Management, 28(1), 58–71. https://doi.org/10.1016/j.jom.2009.06.001

Forbes-Pitt, K. (2011). The assumption of agency theory. ProQuest E-book Central https://ebookcentral.proquest.com.ezproxy.library.strathmore.edu

Francis, P. & Butler, S. (2010). Cutting the cost of insurance claims and taking control of the process. Retrieved from http:www.booz.com.

Frees, E. (2015). Analytics of Insurance Markets. Annual Review of Financial Economics, 7, 253-277. Retrieved May 22, 2021, from http://www.jstor.org/stable/44864038

Gaikwad, L., & Sunnapwar, V. (2020). An integrated Lean, Green and Six Sigma strategies: A systematic literature review and directions for future research. The TQM Journal, 32(2), 201-225. https://doi.org/10.1108/TQM-08-2018-0114

Gandhi, J., Thanki, S., & Thakkar, J. J. (2021). An investigation and implementation framework of Lean Green and Six Sigma (LG&SS) strategies for the manufacturing industry in India. The TQM Journal, 3(7), 89-98. https://doi.org/10.1108/TQM-12-2020-0289

Garza-Reyes, J. A. (2015). Green lean and the need for Six Sigma. International Journal of Lean Six Sigma, 6(3), 226-248. https://doi.org/10.1108/IJLSS-04-2014-0010

Gatzert, N., & Kolb, A. (2014). Risk Measurement and Management of Operational Risk in Insurance Companies from an Enterprise Perspective. The Journal of Risk and Insurance, 81(3), 683-708. http://www.jstor.org/stable/24548086

Gatzert, N., & Wesker, .H (2012). A Comparative Assessment of Basel II/III and Solvency II. The Geneva Papers on Risk and Insurance. Issues and Practices, July 2012, Vol. 37, No. 3, Special Issue on Insurance and Finance (July 2012), pp. 539-570. http://www.jstor.org/stable/41953193

Girling, P. (2013). Operational Risk Management. A complete guide to a successful operational risk framework. John Wiley & Sons, Inc. New Jersey.

Githecha, D. K. (2013). The effect of fraud risk management on the financial performance of commercial banks in Kenya. MSC Project, University of Nairobi

Goel, C. (2013). Insurance claims management: improving staff capacity using BPM. London: Cognizant Business Consulting.

Gollier, C. (2003). To Insure or Not to Insure? An Insurance Puzzle. The Geneva Papers on Risk and Insurance Theory, 36, 414-439.

Grandfield, A. (2005). Operational Risk Management – The View from the Trenches. Operational Risk. Practical Approaches to Implementation. Risk Books: Division of Incisive Financial Publishing Ltd, Haymarket.

Greymyr, I., & Fouquet, J. (2012). Design for Six Sigma and lean product development. International Journal of Lean Six Sigma, 3(1), 45-58. https://doi.org/10.1108/20401461211223722

Hage, J. (1965). An Axiomatic Theory of Organizations. Administrative Science Quarterly, 10(3), 289-320. Doi: 10.2307/2391470

Handbook of Work and Organizational Psychology: Organizational psychology. (1998). United Kingdom: Psychology Press.

Hao, C. (2013). ARMS: An Advanced Operational Risk Management System for Commercial Banks. Third International Conference on Intelligent System Design and Engineering Applications, pp. 386-389, doi: 10.1109/ISDEA.2012.96.

Hain, S. (2009). Managing Operational Risk: Incentives for reporting and disclosure. Journal of Risk Management in Financial Institutions, 2(3), 284-300. Henry Stewart Publications.

Haubenstock, M. (2003). The operational risk management framework. Operational Risk. Regulation, Analysis and Management. Pearson Education Ltd. Harlow.

Heep-Altiner M. , (2018) Introduction. In: Heep-Altiner M., Mullins M., Rohlfs T. (eds) Solvency II in the Insurance Industry. Contributions to Management Science. Springer, Cham. https://doi.org/10.1007/978-3-319-77060-4_1

Hemrit, W. & Ben Arab, M. (2012). The determinants of frequency and severity of operational losses in Tunisian insurance industry. Journal of Risk Finance, 13(5), 438-
475. https://doi.org.ezproxy.library.strathmore.edu/10.1108/15265941211273759

Hoffman, W. (2002). Personal Jurisdiction Over Alien Insurance Companies: The Territory of Coverage Rule. Tort and Insurance Law Journal, 26(4), 703-719. http://www.jstor.org/stable/25762288

Ingram, D.N. (2006). Standard and Poor's Enterprise Risk Management Evaluation of Insurers. Risk Management Journal, 3(7), 14–17.

Insurance Industry Release Report. (2021). https://www.ira.go.ke/images/quartelyreports/2021/Quarter%204%202021%20-Insurance%20Industry%20Release.pdf

Insurance Regulatory Authority (IRA). (2017). Insurance Industry Report - January to December 2017. Nairobi: Insurance Regulatory Authority (IRA).

Insurance Regulatory Authority (IRA). (2020). Insurance Industry Report - January to June 2020. Nairobi: Insurance Regulatory Authority (IRA).

Insurance Regulatory Authority (IRA). (2020). 2020 Annual Insurance Industry Statistics https://www.ira.go.ke/index.php/publications/statistical-reports/annual-reports?id=304

Insurance Regulatory Authority (IRA). (2021). Licensed Insurance Companies 2021. https://www.ira.go.ke/images/LICENCED-INSURANCE-COMPANIES-2021.pdf

International Association of Insurance Supervisors. (2020). Bloomberg.

Iyede, R., Fallon, E. F., & Donnellan, P. (2018). An exploration of the extent of Lean Six Sigma implementation in the West of Ireland. International Journal of Lean Six Sigma, 9(3), 444-462. https://doi.org/10.1108/IJLSS-02-2017-0018

Jacob, T. (2007). Claims processing: Meeting the challenges of today and tomorrow. Whitepaper. UK: Microsoft Corporation.

Jayanthi, N., Kala, I., Sunantha, P. S. & Sukra, A. Vehicle Insurance Calculator Using Augmented Reality. 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), pp. 766-770, doi: 10.1109/ICACCS.2019.8728395.

Jensen, M.C. (1983). Organization theory and methodology. Accounting Review, 56 (2), pp. 319-338.

Johnson, B. M. (2006). Integrated Risk Management among Insurance Companies. New York, Pearson Education Inc.

Jorion, P. (2010). Risk Management. Annual Review of Financial Economics, 2, 347-365. Retrieved May 20, 2021, from http://www.jstor.org/stable/42940221

Kawulich, Barbara. (2004). Qualitative Data Analysis Techniques. https://www.researchgate.net/publication/258110388_Qualitative_Data_Analysis_Techniques

King, E. D. (2001). Integrated Risk Management Systems around the world. New York, Pearson Education.

Koon Lee, K., Ree, S. & Park, Y. H. (2005). A Study of Lean DFSS through the Creative Value Design. Asian Journal on Quality, 6(3), 121-131. https://doi.org/10.1108/15982688200500026

Kothari, C. R. (2012). Research Methodology: Methods and Techniques, New Delhi: New Age Publications.

Krishnan, B. (2010). Claims management and claims settlements in life insurance. The Journal of Insurance Institute of India, 36, 49-57.

Kirikkaleli, D., Yaylali, P., & Safakli, O. V. (2020). The Perception and Culture of Operational Risk in the Banking Sector: Evidence from Northern Cyprus. SAGE Open. https://doi.org/10.1177/2158244020963587

Lam, J. (2014). Operational Risk Management. In Enterprise Risk Management, J. Lam (Ed.). https://doi.org.ezproxy.library.strathmore.edu/10.1002/9781118836477.ch14

Li-Jie, C., Li-Jun, L., & Zhi-Xiang, L. (2009). The research on the early-warning system model of Operational Risk for commercial banks based on BP Neural Network analysis. International Conference on Machine Learning and Cybernetics, pp. 2739-2744, doi: 10.1109/ICMLC.2009.5212096.

Linh, Do & Luong, Thi & Nguyen, Xuan. (2019). Credit Scoring Application at Banks: Mapping to Basel II. Journal of Social and Political Sciences. 2. 10.31014/aior.1991.02.01.51.

Lawrence, P., & Lorsch, J. (1967). Differentiation and integration in complex organizations. Administrative Science Quarterly, 12, 1-30.

Manning, S. and Gurney, A. (2005), "Operational risk within an insurance market", Journal of Financial Regulation and Compliance, Vol. 13 No. 4, pp. 293-300. https://doi.org.ezproxy.library.strathmore.edu/10.1108/13581980510635528

Marshall, R. V. (2000). Integrated Risk Management Systems around the world. New York, Pearson Education.

Michael, K. (2008). The increasing importance of claim management to insurers. The National Underwriter Company.

Miles, J. A. (2012). Management and organization theory: A jossey-bass reader. ProQuest E-book Central https://ebookcentral.proquest.com.ezproxy.library.strathmore.edu

Mishra, M.N. (2018). Identify critical success factors to implement integrated green and Lean Six Sigma. International Journal of Lean Six Sigma, 4(2), 73-77. https://doi.org/10.1108/IJLSS-07-2017-0076

Mitra, S., Palmer, M., Mont, D., & Groce, N. (2016). Can households cope with health shocks in Vietnam? Health Economics, 25 (7), 888–907.

Mitchell, R. & Meacheam, D. (2011). Knowledge worker control: understanding via principal and agency theory. The Learning Organization, 18 (2), pp. 149-160.

Montgomery, D. C. (2010). A modern framework for achieving enterprise excellence. International Journal of Lean Six Sigma, 1(1), 56-65. https://doi.org/10.1108/20401461011033167

Mugenda, O. M., & Mugenda, A., G. (2003). Research methods quantitative and qualitative approaches: Nairobi. Applied Research and Training Services Press.

Mwashi, M. (2017). Implication of Fraud on the Competitiveness of Insurance Companies in Kenya. Unpublished MBA Thesis, University of Nairobi, Nairobi, Kenya

Neale, F., Drake, P., & Konstantopoulos, T. (2020). InsurTech and the Disruption of the Insurance Industry. Journal of Insurance Issues, 43(2), 64-96. Retrieved May 22, 2021, from https://www.jstor.org/stable/26931211

Njegomir, V. (2011). Importance and current issues in agricultural insurance in Serbia, Savremena poljoprivreda, 60(1-2), 38-45.

Nyaga, E. W. (2018). Insurance Fraud Risk Management Practices and Performance of Motor Vehicle Underwriting Companies in Kenya. Unpublished MBA Thesis, University of Nairobi, Nairobi, Kenya

Nyenrode, H. D. (2017). Differentiation and integration in complex organizations. Administrative Science Quarterly, 12, 1-30.

Ohando, R. O. (2015). Relationship between Fraud Risk Management Practices and Financial Performance of Commercial Banks in Kenya. Master of Science in Finance Research Project, Department of Finance. Nairobi: University of Nairobi.

Olson, D. L., & Wu, D. D. (2008). Enterprise Risk Management. World Scientific Publishing Co. Pty. Ltd. Singapore.

Omasete, C. A. (2014). The Effect of Risk Management on Financial Performance of Insurance Companies in Kenya, Unpublished MBA thesis, University of Nairobi.

Orodho, J. (2008). Techniques of Writing Research Proposals and Reports in Education and Social Sciences. (311d ed.). Nairobi: Kanezja HP Enterprises, Maseno.

Oscar, J. A., Sackey, F. G., Amoah, L., & Frimpong, R. (2013). The Financial Performance of Life Insurance Companies in Ghana. The Journal of Risk Finance, 14(3), 161-176. http://dx.doi.org/10.1108/JRF-11-2012-0081

Panda, B., & Leepsa, N. M. (2017). Agency theory: Review of Theory and Evidence on Problems and Perspectives. Indian Journal of Corporate Governance, 10(1), 74–95. https://doi.org/10.1177/0974686217701467

Paulo, A, & Mary, M. (2014). Benchmarking Six Sigma implementation in service companies operating in emerging economies.

Pakurár, M., Haddad, H., Nagy, J., Popp, J., Oláh, J. (2019). The service quality dimensions that affect customer satisfaction in the Jordanian banking sector. Sustainability (MDPI), 11, Article 1113.

Peters, Gareth & Targino, Rodrigo & Shevchenko, Pavel. (2013). Understanding Operational Risk Capital Approximations: First and Second Orders. Journal of Governance and Regulation (print). 2. 58-78. 10.22495/jgr_v2_i3_p6.

Power, R. T. (2006). Integrated Risk Management Systems around the world. New York, Pearson Education.

PricewaterhouseCoopers (PwC). (2017). Digital Case Study: Using Blockchain to transform insurance claims. UK: United Kingdom.

Rao, A. (2007). Evaluation of Enterprise Risk Management (ERM) in Dubai: An Emerging Economy. Risk Management, 9(3), 167-187. Retrieved May 22, 2021, from http://www.jstor.org/stable/4500411

Rejda, E. G. (2003). Principles of Risk management and Insurances. New York, Pearson Education Inc.

Regulation Art. 4(52) (2013, June 26). Regulation 575/2013/EU of the European Parliament and of the Council. Official Journal of the European Union.

Rose, S. (2013). Predicting claims processing: Transforming the insurance claims life cycle using analytics. SAS Whitepaper, 1-8.

Rowe, W. (1982). Two Criticisms of the Agency Theory. Philosophical Studies: An International Journal for Philosophy in the Analytic Tradition, 42(3), 363-378. Retrieved May 20, 2021, from http://www.jstor.org/stable/4319564

Rusanov, Y. Y., Natocheeva, N. N., Belyanchikova, T. V., & Bektenova, G. S. (2017). Project lending in banking risk management. Project lending in banking risk management, 20(4B), 453-471.

Sanlam (2020). Resilience Annual Report and Financial Statements. https://www.sanlam.co.za/kenya/Documents/SANLAM-ANNUAL-REPORT-KENYA-PLC.pdf

Sarmah, S. S. (2018). Understanding Blockchain technology. Computer Science and Engineering, 8(2), 23-29.

Sandner, K., Sieber, S., Tellermann, M., & Walthes, F. (2020). A Lean Six Sigma Framework for the insurance industry: insights and lessons learned from a case study. Journal of Business Economics, 5(6), 46-57.

Saunders, M., Lewis, P., & Thornhill, A. (2014). Research methods for business students (7th Ed). Pitman Publishing.

Saunders, M., Lewis, P. & Thornhill, A. (2016). Research Methods for Business Students. Edinburg Prentice Hall

Scandizzo, S. (2005). Risk Mapping and Key Risk Indicators in Operational Risk Management. Economic Notes, 34: 231 256. https://doi.org.ezproxy.library.strathmore.edu/10.1111/j.03915026.2005.00150.x

Searle, I. (2008). Enterprise Risk Management. London: Spiramus Press.

Sekaran, U. & Bougie, R. (2013). Research Methods for Business: A Skill-Building Approach. 6th Edition, Wiley, New York.

Shiller, J. (2006). The impact of insurance fraud detection system. Journal of Insurance Claims, 8(5), 244-251.

Shiu, Y. (2014). Determinants of United Kingdom general insurance company performance. British Actuarial Journal, 10(5), 1079-1110.

Siddiqui, D. M., & Sharma, T. G. (2010). Measuring the customer perceived service quality for life insurance services: An empirical investigation. International Business Research, 3(3).

Singh, V. (2012). Global trends in non-life insurance: claims. Capgemini.

Siniša, H., Dragan, P., Ivan, F. & Marijan, M. (2015). Telematics System in Usage Based Motor Insurance. Procedia Engineering, Volume 100, Pages 816-825, ISSN 1877-7058, https://doi.org/10.1016/j.proeng.2015.01.436

Smyth, R. (2004). Exploring the Usefulness of a Conceptual Framework as a Research Tool: A Researcher's Reflections. Issues in Educational Research, Vol. 14.

Sofiane, D. (2020). Risk Management as a Method of Translation Criticism. International Journal of Linguistics and Translation Studies, 1(1), 64–71. https://doi.org/10.36892/ijlts.v1i1.17

Swenson, K. (2003). A qualitative operational risk framework: guidance, structure and reporting. Operational Risk. Regulation, Analysis and Management. Pearson Education Ltd, Harlow.

Tennant, G. (2001). Six Sigma: SPC and TQM in Manufacturing and Services. Hampshire: Gower Publishing Company

TIBCO (2011). Dynamic Claims Processing. USA: TIBCO Software Inc

Tlapa, D., Limon, J., García-Alcaraz, J.L., Baez, Y. & Sánchez, C. (2016). Six Sigma enablers in Mexican manufacturing companies: a proposed model. Industrial Management & Data Systems, 116(5), 926-959. https://doi.org/10.1108/IMDS-06-2015-0265

Thomas, A., Barton, R., & Chuke-Okafor, C. (2009). Applying lean six sigma in a small engineering company: a model for change. Journal of Manufacturing Technology Management, 20(1), 113-129. https://doi.org/10.1108/17410380910925433

Torre-Enciso, M. I. M., & Barros, R. H. (2013). Operational risk management for insurers. International Business Research, 6(1), 1-2.

Tripp, M., Bradley, H., Devitt, R., Orros, G., Overton, G., Pryor, L., & Shaw, R. (2004). Quantifying Operational Risk in General Insurance Companies. British Actuarial Journal, 10(5), 919-1026. http://www.jstor.org/stable/41141661

Tseng, C. (2007). Internal Control, Enterprise Risk Management, and Firm Performance. Unpublished PhD Dissertation. Department of Accounting and Information Assurance. Robert H. Smith School of Business

Wenk, D. (2005). Risk Management and Business Continuity, Overview and Perspective. Journal of the Chartered Insurance Institute, 3(3), 234-246.

Wesley, K. W. (2004). The Fraud Management Life Cycle Theory: a holistic approach to fraud management. Journal of Economic Crime Management, 6(4), 74-89.

Woods, M. (2009). A contingency theory perspective on the risk management control system within Birmingham City Council. Management Accounting Research, 20(1), 69-81. https://doi.org/10.1016/j.mar.2008.10.003

Yang, S. Y, Li, H. A, & Fang, H. C. (2017). The Non-linear relationship between economic and life insurance development in Asia: A panel threshold regression analysis. Computer Science and Its Applications - Ubiquitous Information Technologies. 330(20):1281-1290.

Young, J. (2014). Operational Risk Management. 2nd Edition. Pretoria. Van Schaik Publishers.

Yusuf, T.O., & Dansu, F. S. (2014). Effect of claim cost on insurers' profitability in Nigeria. International Journal of Business and Commerce, 3(10), 1-20

APPENDICES

Appendix 1: Differences between Basel II/III and Solvency II

	Basel II/III	**Solvency II**
Pillar 1	Calculation of Minimum Capital Requirement (MCR) using the measures stated in Figure 2.4. Value at risk is considered only for market risk capital requirement, operational risk is viewed comparatively to measures for credit risk. Does not account for aggregation or interdependence of risks.	Two-pronged approach requiring; Minimum Capital Requirement (MCR) covered by basic own funds i.e., market value liabilities – market value of assets. 99.5% confidence level required for the insurer as a whole, accounting for interdependencies and aggregate losses, and inclusion of Solvency Capital Requirements (SCR) that is an additional amount of capital held to absorb unexpected losses from all risk classes.
Pillar 2	Supervisory process that strengthens and encourages efficient and advancement of risk management in order to maintain capital adequacy (Nadine & Wesker, 2012)	Includes discussion on strategies, processes and reporting procedure, and valuation of technical provisions, assets and own funds (Gazert & Wesker, 2012). Robust internal enterprise-wide risk management framework that includes Own Risk Solvency Assessment (ORSA).
Pillar 3	Public disclosure for consolidated top level and for the separate risk types; credit market, and operational risk.	Public disclosure of individual entities of a group, as well as disclosure or both MCR and SCR for the enterprise as a whole. This also includes description of business and performance as well as differences in assumptions underlying the standard calculation for SCR and institution's individual risk profile (Gazert & Wesker, 2012).

Appendix 2: Interview Schedule

Introduction

Good morning/afternoon, my name is Emma Ikonge a student at Strathmore University, Business School pursuing a Master of Development Finance. I am currently conducting a study to develop a Framework for Monitoring Operational Risks in Claims Processing. Your feedback will be used to help in the design and development of the proposed framework.

Be informed that all information shared with me will be handled with utmost confidentiality. The interview will take about 15-20minute of your time.

Kindly indicate if you will wish to continue with this interview.

Yes – want to continue > continue with the interview

No – do not want to continue > terminate interview

Biography

1. Please indicate your gender
   - ☐ **Male**
   - ☐ **Female**
2. Please indicate your department
   - ☐ **Internal Audit and Risks**
   - ☐ **Finance**
   - ☐ **Claims Manager**
3. How long have you been involved in claims management?
   - ☐ **0-12 Months**
   - ☐ **1-2 years**
   - ☐ **More than 2 years**

A). Operational risks associated with the claims processing

A1. Please indicate how you have categorised the operational risks indicators in your department based on Tripp (2004) proposition of categorising risk indicators, that is,

1. Exposure related indicators
2. Loss related indicators

3. Cause-related indicators

A2. How are the exposure related indicators which are described to be volume-based indicators that allow measurement throughout processes likely to lead to operational failure? How do the following exposure related indicators apply to your department?

- Staff turnover
- Complaints

A3. Loss related indicators measure events associated with operational losses and are considered lagging indicators hence insufficient alone. How do the following loss related indicators manifested in your department?

- Errors
- Fraudulent activities
- Unauthorised activities
- Security breaches
- Misuse of data

A4. Cause-related indicators measure factors identified as drivers for operational losses and are leading indicators. In your department how prevalent are these indicators: IT failure, Regulatory changes and Economic downturn?

A5. What will you say is the degree of occurence of the following operational risks: Fraud, Human Errors, Accounting Errors, System Failure and Statutory reporting failure in your department?

A6. How do you describe and rank the impact of the following operational risks in your department?

Operational Risk	**Rank**
Fraud	
Human Errors	
Accounting Errors	
System Failure	
Statutory reporting failure	

A7. Is there an objective criteria for ranking the risks in A6? Briefly explain it.

B). Information communication technology utilization in monitoring operational risks

Has your department adopted ICT? **Yes** ☐ **No** ☐

B1. Please indicate the role played by ICT in operational risk management in your department?

C). Application of Blockchain technology for monitoring operational risks in the claims processing in insurance

C1. Blockchain is a new technology that is changing the way records are managed. Has your department considered adopting it? ☐ **Yes** **No** ☐

C2. The following are the characteristics of Blockchain technology, please indicate a characteristic that your department will consider important for your operations.

1. **Consensus** (Emphasises that for a transaction to be accepted and recorded on the Blockchain, all the participants must agree to follow the same rules).

2. **Provenance** (focuses on the participants knowing where the assets came from and how its ownership has changed over time-traceable property).

3. **Immutability** (No participant can modify a transaction after it has been recorded on the ledger).

4. **Finality** (In a Blockchain network, there is only one source of truth. There is only one ledger for the whole network).

Please explain why you have selected the above characteristic.

Thank you very much for your participation and I would like to highlight as mentioned above, that all data collected will be confidential.

Warmest Regards,

Emma Ikonge

Appendix 3: Questionnaire

Introduction

Good morning/afternoon, my name is Emma Ikonge, a student at Strathmore University, Business School pursuing a Master of Development Finance. I am currently conducting a study to develop a Framework for Monitoring Operational Risks in Claims Processing. Your feedback will be used to help in the design and development of the proposed framework.

All information shared with me will be handled with utmost confidentiality.

Kindly indicate if you will wish to continue with responding to this questionnaire by ticking against the response below:

Are you willing to participate in this study?

Yes – > continue to respond to the questions

No – > Do not continue to respond to the questions

Biography

1. Please indicate your gender
   - ☐ **Male**
   - ☐ **Female**
2. Please indicate your department
   - ☐ **Risks & Compliance**
   - ☐ **Internal Audit**
   - ☐ **Finance**
   - ☐ **Claims Manager**
   - ☐ **Premium Administration**
   - ☐ **Underwriting**
   - ☐ **IT**
3. Please indicate your position in the organisation
   - ☐ **Head of department**
   - ☐ **Manager**

☐ **Officer**

4. How long have you been involved in claims management?

☐ **0-12 Months**

☐ **1-2 years**

☐ **More than 2 years**

Section B: Claim processing operations

Do you agree that the following claim processing operations are conducted in your company regularly as per laid down procedures? (Tick the box that applies).

Claim Processing operation	**Agree**	**Neutral**	**Disagree**
Filing of loss			
Registering and documentation of claim			
Risk Assessment and adjustment			
Communication of risk assessment report			
Claim settlement and payment			

Section C: Operational Risk indicators

Please indicate the extent you agree how are the following operational risk indicators manifest in your company

Operational Risk Indicators	**Strongly agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
Human Errors					

Fraudulent activities					
Staff turnover					
Security breaches					
Misuse of data					
Unauthorised activity					
IT systems failure					
Client complaints					

Section D: Information communication technology used to monitor operational risks

Please indicate by selecting the box the level of utilization of IT systems in the claim processing operations in your company. Use the levels 3 being high when completely using IT systems, 2 being moderately using IT and 1 being not using IT at all.

Claim Processing operation	**1**	**2**	**3**
Filing of loss			
Registering and documentation of claim			
Risk Assessment and adjustment			
Communication of risk assessment report			
Claim settlement and payment			

Section E: Framework for monitoring operational risks that uses Blockchain technology

Please rank the characteristic(s) of the Blockchain that your department will consider important for your operations. Use the rank 1 being not important, 2 being neutral and 3 being important

Blockchain characteristic	**1**	**2**	**3**
Consensus (Emphasizes that for a transaction to be accepted and recorded on the Blockchain, all the participants must agree to follow the same rules)			
Provenance (focuses on the participants knowing where the assets came from and how its ownership has changed over time-traceable property)			
Immutability (No participant can modify a transaction after it has been recorded on the ledger).			
Finality (In a Blockchain network, there is only one source of truth. There is only one ledger for the whole network).			

Section F: Types of operational risks

Indicate how likely are the following operational risks to occur in your company based on your recent experience considering the operational risk indicators

Operational Risk Indicators	**Strongly agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
Fraud					
Human error					

Accounting errors					
IT System failure					
Statutory reporting failure					

Thank you very much for your participation and I would like to highlight as mentioned above, that all data collected will be confidential.

Warmest Regards,

Emma Ikonge

Appendix 3: NACOSTI Permit

REPUBLIC OF KENYA

NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Ref No: 859794

Date of Issue: 23/August/2021

RESEARCH LICENSE

This is to Certify that Ms.. Emma Ikonge Maraga of Strathmore University, has been licensed to conduct research in Nairobi on the topic: A Framework for Blockchain Technology in the Monitoring of Operational Risks in Claims Processing for Saulam Insurance for the period ending : 23/August/2022.

License No: NACOSTI/P/21/12361

859794

Applicant Identification Number

Director General
NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Verification QR Code

NOTE: This is a computer generated License. To verify the authenticity of this document, Scan the QR Code using QR scanner application.

THE SCIENCE, TECHNOLOGY AND INNOVATION ACT, 2013

The Grant of Research Licenses is Guided by the Science, Technology and Innovation (Research Licensing) Regulations, 2014

CONDITIONS

1. The License is valid for the proposed research, location and specified period
2. The License any rights thereunder are non-transferable
3. The Licensee shall inform the relevant County Director of Education, County Commissioner and County Governor before commencement of the research
4. Excavation, filming and collection of specimens are subject to further necessary clearence from relevant Government Agencies
5. The License does not give authority to tranfer research materials
6. NACOSTI may monitor and evaluate the licensed research project
7. The Licensee shall submit one hard copy and upload a soft copy of their final report (thesis) within one year of completion of the research
8. NACOSTI reserves the right to modify the conditions of the License including cancellation without prior notice

National Commission for Science, Technology and Innovation
off Waiyaki Way, Upper Kabete,
P. O. Box 30623, 00100 Nairobi, KENYA
Land line: 020 4007000, 020 2241349, 020 3310571, 020 8001077
Mobile: 0713 788 787 / 0735 404 245
E-mail: dg@nacosti.go.ke / registry@nacosti.go.ke
Website: www.nacosti.go.ke