

**OPERATIONAL RISK CONTROL MEASURES FOR THE LESOTHO BANKING
INDUSTRY TO MANAGE A CRISIS EVENT: A CASE STUDY OF COVID-19**

by

MATOKELO MOTOPI

submitted in accordance with the requirements

for the degree of

MASTER OF COMMERCE

in the subject

BUSINESS MANAGEMENT

at the

DEPARTMENT OF FINANCE, RISK MANAGEMENT AND BANKING

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROF J YOUNG

June 2024

DECLARATION


Name: Matokelo Motopi

Student number: 60018712

Degree: Master's in Business Management

Operational risk control measures for the Lesotho banking industry to manage a crisis event: A case study of covid-19

I declare that the above dissertation is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.



SIGNATURE

19/06/2024

DATE

ACKNOWLEDGEMENTS

I give thanks to God for guiding me on this quest. Without his grace, I could not have finished this thesis. His mercy on me gave me bravery, strength, wisdom, and patience. In addition, I would like to thank Prof. Jackie Young, my supervisor, for his dedication, hard work, and commitment that significantly contributed to this outcome. Prof Young has enormously enhanced my abilities and comprehension. Additionally, I appreciate my work supervisors for their understanding, support and perseverance. I also like to thank Mr. Khobotlo for assisting me with this study's statistical analysis. Your tenacity, wisdom, and assistance are greatly valued. Ms Tshegofatso SehloDIMELA, thank you for your outstanding editorial services. I am grateful to everyone including friends, family, and colleagues for their support in all forms. I assure you that although I may be claiming credit for finishing this thesis, it would not have been possible without your support.

ABSTRACT

Banks are essential to any economy because they play an important role in ensuring financial stability. Thus, it is critical that banks always remain functional to be profitable and ensure the country's economic progress. The COVID-19 pandemic has had an impact on the economies of many countries, especially on the banking industry of those countries. Thus, the pandemic had the potential to trigger economic crises. It is therefore important that banks plan to prepare for crisis events that could disrupt normal operations and expose them to operational risks. The pandemic revealed many shortcomings in risk control measures for banks to continue to function as critical entities in an economy. This study aims to identify operational risk control measures that may be applicable for preparing banks to address crisis events. These risk control measures were identified from the literature review in a quest to investigate the impact of the COVID-19 pandemic on operational risks faced by banks. The objective was to identify operational risk control measures for the Lesotho banking industry to prepare for future crisis events. The study identified a list of operational risk control measures relevant to a potential crisis event. These control measures were subjected to an empirical analysis to determine their importance and current applicability. Using a closed-ended questionnaire, the study collected the data for statistical analysis. The descriptive and inferential results confirmed that all the identified operational risk control measures are important for ensuring a bank's preparedness for a potential crisis event. However, although the control measures were rated as currently applicable by the banks, not all of them were adequately implemented. The study recommends that banks develop and implement the risk control measures to adequately prepare for potential crisis events.

Keywords: Operational risk, risk management framework, operational risks management process, operational risk control, crisis events.

KAKARETSO

Libanka li bohlokoa moruong ofe kapa ofe mme li bapala karolo ea bohlokoa ho netefatsa botsitso ba lichelete. Ka lebaka leo, ho bohlokoa hore libanka li lule li sebetsa molemong oa ho boloka phaello le ho netefatsa tsoelo-pele ea moruo oa naha. Leha ho le joalo, seoa sa covid-19 se bile le tšusumetso moruong oa linaha tse ngata mme se bile le monyetla oa ho baka mathata a moruo a ka amang lekala la libanka. Ka lebaka leo, ho bohlokoa hore libanka li rera esale pele ho itokisetša liketsahalo tsa tlokotsi. Liketsahalo tsa likoluoa li ka 'na tsa senya ts'ebetso e tloaelehileng ea banka, ho pepesa libanka kotsing ea ts'ebetso. Lingoliloeng li ile tsa hlahlojoa e le hore ho khethoe mabaka a kotsi a ts'ebetsong ao libanka li ka 'nang tsa pepeseha ho tsona le ho hlalosa mehato e nepahetseng ea ho laola kotsi. Boithuto bo tsoetse pele ho hlahloba phello ea seoa sa covid-19 kotsing ea ts'ebetso ea banka. Sepheo e ne e le ho hloaea mekhoha ea taolo ea kotsi eo indasteri ea libanka ea Lesotho e ka e sebelisang molemong oa ho itokisetša likoluoa tse tlang, tse entseng tlhahlobo e matla ea boithuto bona. Libanka tse tharo ho tse hlano tsa Lesotho li kenyelelitsoe datha tsa mohlala. Ts'ebetso ea banka e bohareng ke e 'ngoe ea tsona. Palo ea baahi e kenyelelitse ba arabetseng ba 41 ho tsoa libankeng tse tharo. Lintlha tse fumanoeng li ile tsa bapisoa ho sebelisoa phuputso, 'me mofuputsi o ile a leka ho koala lekhalo pakeng tsa bohlokoa ba libanka ho kenya ts'ebetsong litsamaiso tse bontšitsoeng tsa kotsi le ts'ebetsong ea hona joale ea litsamaiso ho bonts'a liphello tse hlalolang le tse fokolang. Mehato eohle e tiisitsoeng ea taolo ea kotsi e bohlokoa ebile e sebelisitsoe libankeng; leha ho le joalo, ho bonahala ho na le lekhalo ts'ebelisong ea litsamaiso. Tlhahlobo e bonts'a taolo ea bohlokoa ea ts'ebetso ea likotsi tseo libanka li ka li sebelisang ho itokisetša mathata le ho netefatsa tsoelo-pele ea khoebo ha ho ka ba le mathata.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS	ii
ABSTRACT	iv
KAKARETSO	v
LIST OF ABBREVIATIONS	xi
LIST OF FIGURES	xii
LIST OF TABLES	xiii
CHAPTER 1: INTRODUCTION	14
1.1. Background	14
1.2. Origin of the COVID-19 Pandemic.....	14
1.2.1. Earnings and profitability	15
1.2.2. Capital adequacy.....	17
1.3. Risk Management	17
1.4. Operational Risk in the Banking Industry	19
1.4.1. Basel II.....	21
1.5. Problem Statement	22
1.5.1 Purpose of the study	23
1.5.2 Objectives	23
1.6. Research Methodology	24
1.6.1 Research paradigms	24
1.6.2. Research approach and design	24
1.6.3. Data collection	25
1.6.4. Data analysis	26
1.6.5. Data measurement.....	26
1.6.6. Validity and reliability.....	26
1.6.7. Generalisation	27
1.6.8. Sampling and population.....	27
1.7. Ethical Clearance	27
1.7.1 Informed consent.....	28
1.7.2. Deception.....	28
1.7.3. Privacy, confidentiality, and anonymity	28
1.7.4. Coercion, incentives, and sensitive information	28

1.7.5. Permission	28
1.8. Limitations and Delimitations	28
1.9. Structure of the Study	28
CHAPTER 2: LITERATURE REVIEW ON OPERATIONAL RISK MANAGEMENT	30
2.1 Introduction	30
2.2. Defining Risk Management	30
2.3. Risk Management Framework	32
2.3.1. COSO risk management framework	33
2.3.2. ISO 31000 risk management framework	35
2.3.3. RMA risk management framework	36
2.3.4. Concluding remarks	37
2.4. Components of an Operational Risk Management Framework	37
2.4.1. Risk culture	37
2.4.2 Risk governance structures	38
2.4.3 Risk management strategy	40
2.4.4. Risk management process	42
2.5. Operational Risk	56
2.5.1 Operational risk definition	56
2.5.2. Process risk	57
2.5.3. People risk	59
2.5.4. System risk	60
2.5.5. External factors	62
2.6. Summary of Operational Risk	64
2.7. Conclusion	64
CHAPTER 3: IMPACT OF COVID-19 ON OPERATIONAL RISK FACTORS	68
3.1. Introduction	68
3.2. People Risk	68
3.3. Process Risk	69
3.4. Systems Risk	70
3.5. External Risks	72
3.5. Conclusion	73
CHAPTER 4: RESEARCH DESIGN AND METHODOLOGY	76

4.1. Introduction	76
4.2. Research Design	76
4.2.1. Descriptive research	76
4.2.2. Exploratory research	77
4.2.3. Explanatory design	77
4.3. Research Philosophy/Paradigm	78
4.3.1. Positivism	79
4.3.2. Post positivism	79
4.3.3. Interpretivism	79
4.3.4. Realism	80
4.3.5. Pragmatism	80
4.4. Research Approach	80
4.4.1. Deductive approach	81
4.4.2. Inductive approaches	81
4.4.3. Abductive approach	81
4.5. Methodological Choice	82
4.5.1. Quantitative research	82
4.5.2. Qualitative research	82
4.5.3. Mixed methods	83
4.6. Research Strategy	83
4.6.1. Experiments	84
4.6.2. Pre-experimental designs	84
4.6.3. True experimental designs	84
4.6.4. Quasiexperimental designs	84
4.6.5. Survey	84
4.7. Time Horizon	85
4.8. Techniques and Procedures	86
4.8.1. Study population	86
4.8.2. Sampling technique	86
4.8.3. Data collection	88
4.9. Data Analysis	90
4.9.1. Data measurement	91

4.9.2. Results of the validity tests.....	94
4.9.3. Ethical considerations	96
4.10 Conclusion	98
CHAPTER 5: DATA ANALYSIS	100
5.1. Introduction	100
5.2. Biographical Information of the Participants	100
5.2.1. Bank departments	101
5.2.2. Focus area.....	102
5.2.3. Years of experience in risk management	102
5.2.4. Years of experience with your organisation	102
5.3. Results Interpretation	103
5.4. Concluding Remarks	138
CHAPTER 6: SUMMARY, CONCLUSIONS AND RECOMMENDATIONS	145
6.1. Introduction	145
6.2. Summary of the Study.....	145
6.3. The Purpose and objectives of the Research.....	146
6.4. The Results of the Survey.....	146
6.4.1. Operational risk control measures	146
6.4.2. Confirmation of the identified risk control measures.....	149
6.4.3. Data analysis	149
6.5. Study Constraints	149
6.6. Recommendations	150
6.7. Research Contribution	155
6.8. Suggestions for Additional Research.....	155
6.9. Chapter Conclusion.....	155
References	156
Annexure A: Questionnaire	176
.....	176
Annexure B: Email cover page for a questionnaire.....	179
Annexure C: Consent form	182
Annexure D: Diagnostic results	183
Annexure E: Reliability calculator	185

Annexure F: Ethical clearance certificate	186
Annexure G: Gate keeper approvals	190
Annexure H: Checklist	218
Annexure I : Confidentiality agreement statistian	221
Annexure J: Descriptive analysis	225
Annexure I: Statistical results	235
Annexure K: Editor certificate.....	238

LIST OF ABBREVIATIONS

CBL	Central Banks of Lesotho
WHO	World Health Organisation
BCBS	Basel Committee on Banking Supervision
GOL	Government of Lesotho
LBFC	Lesotho Building Finance Corporation
IOR	Institute of Operational Risk
COSO	Committee of Organisations of the Treadway Commission
CCDCP	Chinese Centre of Disease Control and Prevention
IMF	International Monetary Fund
FSB	Financial Stability Board
ISO	International Organization for Standardization
ORMF	Operational Risk Management Framework
RMA	Risk Management Association
BCM	Business continuity management plan
PWC	PricewaterhouseCoopers
BCP	Business continuity plan
ISACA	Information Systems Audit and Control Association

LIST OF FIGURES

Figure 2.1: Components of a risk management process	44
Figure 4.1 : Research onion	78
Figure 4.2: Adapted research onion	98
Figure 5.1: Definition of operational risk management	106
Figure 5.2: Operational risk management framework	107
Figure 5.3: Risk culture	108
Figure 5.4: Risk management strategy	110
Figure 5.5: Governance structure	111
Figure 5.6: Risk management process	113
Figure 5.7: Risk identification	114
Figure 5.8: Risk evaluation	115
Figure 5.9 Risk control and mitigation	116
Figure 5.10: Risk monitoring	118
Figure 5.11: Appointing employees for critical functions	119
Figure 5.12: Training of employees	120
Figure 5.13: Health and safety environment	122
Figure 5.14: Policies and procedures	123
Figure 5.15: Communication strategies used during a crisis event	124
Figure 5.16: Business continuity management policy	126
Figure 5.17: Cybersecurity policy	127
Figure 5.18: Communication programme	128
Figure 5.19: Data back-up facilities	129
Figure 5.20. Business continuity management	130
Figure 5.21: Inclusion of all stakeholders in the BCM	131
Figure 5.22: Crisis management	132

Figure 5.23: Business continuity plan (BCP)	133
Figure 5.24 Training drills	134
Figure 5.25: Identifying critical functions	135
Figure 5.26: Remote working.....	137

LIST OF TABLES

Table 1.1: Examples of bank failures	18
Table 4.1: Pilot questionnaire results	94
Table 5.1: Biographical information of the participants	100
Table 5.2: Independent sample t-test for the equality of means.....	103
Table 5.3: Priority of risk control measures	139
Table 5.4: Top 10 risk control measures with the highest variance between importance and current applicability	142
Table 5.3: Identified operational risk controls and their description.....	146

CHAPTER 1: INTRODUCTION

1.1. Background

Banks are crucial to any economy and are significant for maintaining the financial stability of a country's economy. If there are no profits made, then loans and other financial services cannot be provided, depriving the economy of the required credit (Central Bank of Lesotho [CBL] Newsletter, 2020). The Central Bank of Lesotho Newsletter (2020) indicate that Lesotho is known for its slow economic growth and high unemployment, although banks' financial performance improved in 2020.

Similarly, the COVID-19 pandemic has affected the country's economy and triggered an economic crisis, affecting the banking sector in terms of weaknesses and general hardships (Central Bank of Lesotho Annual Report, 2020). Tougher control policies such as lockdowns implemented by countries to curb the spread of COVID-19 are among the hardships that impacted the banking industry (Ozili & Arun, 2020). The shutdown of banking halls also affected the banking industry as an important factor in the economy (Ozili & Arun, 2020). The effects of COVID-19 were anticipated to cause high defaults on loans and lower levels of liquidity in the banking system (Central Bank of Lesotho Financial Stability Report, 2020). This research aims to investigate the impact of the COVID-19 pandemic on operational risks faced by the Lesotho banking industry to identify possible control measures during a crisis event.

This study first reviewed the literature to identify relevant operational risk control measures. The study investigated the origin of the COVID-19 pandemic to determine its impact on the banking industry and the economy.

The next section outlines the source of the COVID-19 pandemic and the measures taken to minimise its spread and provides a brief review of the impact that the pandemic has had on the economy.

1.2. Origin of the COVID-19 Pandemic

In December 2019, the Chinese Centre of Disease Control and Prevention (CCDCP) informed the World Health Organization (WHO) of unknown pneumonia-like cases seen in the Chinese city of Wuhan in Hubei Province (WHO, 2020). Within three months, the virus had spread to more than 118,000 people, causing 4,291 deaths across 114 countries worldwide. This prompted the WHO to declare the disease a global pandemic on 11 March 2020 and named it the COVID-19 pandemic (WHO, 2020).

Initially, it was assumed that the pandemic would be centred in China, but it soon spread to the rest of the world because people were moving from one place to another (WHO, 2020). The first COVID-19 case in India was detected on 30 January 2020 in the State of Kerala (Kumar, 2020). It later emerged that the infected people had a travel history from Wuhan. To

minimise the spread of the virus, numerous measures were taken to stifle economic activities. Measures were introduced to curb the spread of the virus; however, they affected the demand side due to the health risk of going to public places, including shops, restaurants, and hair salons (Eichenbaum, Rebelo & Trabandt, 2022). Individuals had to make daily decisions such as how to manage inventories of staple food, how to consume and save and when to buy or sell stock (Eichenbaum et al., 2022). People were encouraged to practice social distancing, resulting in the complete shutdown of financial markets, corporate offices, businesses, and other social places (Ozili & Arun, 2020).

The economic burden became a major concern. Other industries that were adversely impacted included travel, hospitality, sports, oil-dependent countries, financial markets, entertainment, events, health, education, and the banking industry (Mishra, Sachi Das, Yadav, Khan, Afzal, Alarifi, Kenawy, Ansari, Hasnain & Nayak, 2020). For example, Marinoni, Van, Land and Jenson (2020) state that the health crisis quickly evolved into economic, social, and cultural crises. Baldwin and Maura (2020) note that although the COVID-19 pandemic is contagious, it is also considered economically infectious because the resulting shutdown measures plunged the global economy into severe contraction. The shutdown also had an impact on the financial industry, which hindered economic growth (Ashraf & Goodell, 2022). A well-functioning banking system promotes economic growth by providing liquidity in general and credit allocation in particular (Colak & Öztekin, 2021). Earnings and profitability, as well as capital adequacy, are among the other factors that might contribute to a well-functioning banking system.

1.2.1. Earnings and profitability

Profitability is a company's ability to generate profits from its operations (Correia, Flynn, Uliana, Wormald & Dillon, 2015). It is seen as one of the four blocks for analysing financial statements and a company's overall performance and reflects its operating efficiency, as it is commonly associated with gross, operating, and net profits (Correia et al., 2015). Correia et al. (2015) describe earnings as a company's profits after all expenses have been subtracted.

Al-Harbi (2019) investigates the effect of internal and external variables on the profitability of conventional banks operating in developing and underdeveloped countries and revealed that a bank's profitability can be improved by variables such as equity, foreign ownership, off-balance sheet activities, real gross domestic product (GDP) growth, the real interest rate and concentration. The results further suggest that a bank's profitability can be improved through growing the banking industry and increasing loans. However, it is evident from Al-Harbi (2019) that GDP per capita, market capitalisation and bank size have no impact on a bank's profitability. Other factors that can increase profitability include sound financial assembly,

advanced labour productivity, reduced operating costs, sturdy market power, and economic growth (Yao, Haris & Tariq, 2018). Nonetheless, according to Li, Feng, Zhao and Carter (2021), because of the impact that COVID-19 has had on the economy, credit standards were stiffened, and the demand for many types of loans was reduced, therefore affecting banks' performance as well as risk. According to Khrawish (2011), capital strength is another determinant of banks' profits. Ehiedu (2022) indicates that capital adequacy reduces banks' financing costs, which results in increased profit.

Owing to the strict measures that have been taken by most countries to control the spread of the COVID-19 pandemic, the banking industry has also been affected (Eichenbaum et al., 2022; Ozili & Arun, 2020). The banking industry was affected by extremely low interest rates and disrupted operations (International Monetary Fund [IMF], 2020). Similarly, bank profitability was negatively affected by a decrease in bank operations worldwide, which led to a decrease in transaction fees collected from customers by banks, thus negatively impacting banks' profits (Ozili & Arun, 2020). Therefore, it is evident that external factors such as the COVID-19 pandemic can affect banks' operations and cause a distraction that could affect the normal functioning of the banking industry. Among other factors that affect banking industry operations is service quality because of the unavailability of staff and additional expenditures on operations such as technology (Marcinkowska, Szambelańczyk, J, Szambelańczyk, J.P, & Kulińska-Sadłocha, 2020). In addition to service delivery, sale rates were also negatively affected by restrictive measures taken to control the spread of the COVID-19 pandemic. Movements were restricted, jobs were lost, and businesses were closed, resulting in a loss of income for some people, which exposed banks to operational risks (Ozili & Arun, 2020).

According to Wójcik and Ioannou (2020), the pandemic continues to accelerate changes in human behaviour. Individuals were forced to resort to digital banking, and when all restrictions and social distancing were lifted, people were likely to remain with this type of banking system. This may result in a decrease in sales of other products (Lagoarde-Segot & Leoni, 2013). Nonetheless, individuals' expenditures on services such as medical treatment increased because of the pandemic, and individuals were forced to withdraw their long-term investments as early redemptions to compensate for medical expenditures, loss of income and low profits in businesses. Therefore, bank reserves were drained (Kisa, 2020). When long-term investments are forgone and reserves are drained, the financial sector is likely to experience liquidity problems and potential collapses, which in turn affect banks' cash flow and profitability (Acharya & Steffen, 2020).

Ehiedu (2022) agrees that capital strength is the main determinant of most banks' profitability. Capitalised banks face lower costs of external financing, thus reducing their costs and

enhancing their profits (Yao et al., 2018). The next section addresses the capital adequacy of banks.

1.2.2. Capital adequacy

Capital adequacy is described as a measure of how much a bank has available and is defined as a measurement of a bank's risk-subjective credit exposure (Yao et al., 2018). The Basel Committee on Banking Supervision (BCBS) (2010) states that capital adequacy influences the financial sector's profitability and guarantees that banks have enough capital to protect depositors' money. Olalekan and Adeyinka (2013) refer to adequate capital in banking as an assurance provided to customers that their money is safe and that the bank can meet customers' needs for funding at all times.

Capital is possibly the most important safeguard for banks since it provides the resources to recover from significant losses and ensures depositors that their money is safe (Central Bank of Lesotho, Supervision Report, 2020). Bitar and Tarazi (2022) mention that banks should be able to maintain economic activities during the COVID-19 pandemic because they were well capitalised in the pre-COVID-19 period and because of the eased capital requirements of other countries (Bitar & Tarazi, 2022). For example, the USA, the UK, and Canada temporarily relaxed their countercyclical buffers, while EU countries deferred the implementation of more strict capital rules during the pandemic. To minimise the economic impact of COVID-19, the Government of Lesotho (GOL) proposed certain measures, including loan repayment deferment programmes and interest rate reductions (Central Bank of Lesotho Annual Report, 2020). Furthermore, as a relief to banks, the Central Bank of Lesotho postponed the migration from Basel I to Basel II, as well as the adoption of several Basel III components. Basel II and III would require banks to reserve more capital in addition to the existing minimum requirement. Consequently, deferral was launched to provide additional money to commercial banks to enable them to issue loans to consumers when necessary (Central Bank Supervision Report, 2020). Accordingly, banks would remain liquid and sufficient to meet the financial needs of their consumers.

Contagious diseases such as COVID-19 affect not only future investments but also labour productivity, economic activity, and risk management (Wang, Cheng, Yue & McAleer, 2020). The next section defines risk management, with operational risk, as the focus of this study.

1.3. Risk Management

Chhabra (2013) defines risk management as the submission of a proactive strategy to plan, lead, coordinate, and control various risks to which a business is exposed. Risk has an influence on the goals and overall success of organisations (Chhabra, 2013). Mahendra, Pitroda and Bhavsar (2013) describe risk management as the identification of threats that

could have a negative effect on the performance of the business. Nonetheless, the aim of risk management is not to avoid bearing risks but to evaluate the identified risks so that appropriate mitigations can be developed (Kanchu & Kumar, 2013). Mare (2019) notes that over the years risk management became vital because of several unpleasant incidents, including fraud cases, terrorist attacks and the global financial crises that occurred in 2008. African Bank tragedy is another example of inadequate risk management, demonstrating how vulnerable a bank may be. Table 1.1 below illustrates examples of bank failures due to inadequate risk management.

Table 1.1: Examples of bank failures

Bank	Description	Source
African Investments Limited	The bank collapsed due to governance shortcomings, inadequate risk management, and insufficient accounting procedures, among other things.	(Bloomberg news, 2014)
Allied Bank of Nigeria, Rims Merchant Bank, and Spring Bank	Poor management of enterprise risk.	(Oluwasey, Ahmad, Omar & Ebenezer, 2016).
Lesotho Building Finance Corporation (LBFC)	Poor lending processes.	(Matlanyane & Harmse, 2002)
Lesotho Bank	Poor risk management that resulted in financial problems.	(Matlanyane & Harmse, 2002)
The Agricultural Development Bank	Inadequate financial management.	Matlanyane & Harmse, 2002).

Source: Bloomberg News (2014), Oluwasey, Ahmad, Omar and Ebenezer (2016), and Matlanyane and Harmse (2002).

The trend of bank distress in Nigeria from 1987–2011 shows that one of the main causes of the increase in bank failure in Nigeria is poor management of enterprise risk (Oluwasey et al., 2016). The trend towards poor risk management was also highlighted in a series of bank failures in Lesotho. The collapse of the Lesotho Building Finance Corporation (LBFC) in the late 1970s was a result of poor lending practices (Matlanyane & Harmse, 2002). As a result, the LBFC was forced to merge with the Government Development Bank in 1993, which was at the time called the Lesotho Bank. Despite the merger, Lesotho Bank was liquidated in 2001 due to serious financial problems it had been experiencing since the 1990s. The Agricultural Development Bank was also closed in 1998 because of similar problems (Matlanyane & Harmse, 2002).

According to the BCBS (2010), even though risk is inherent to the banking system, banks still take risks to increase their profit margins. According to Heffernan (2005), risk can be grouped into the following eight types:

- Credit risk.
- Counterparty risk.
- Liquidity risk.
- Settlement risk.
- Market risk.
- Operational risk.
- Capital risk.
- Political risk.

According to Apostolik, Donohue and Went (2009), operational risk is among the greatest risks faced by banks and is also recognised by the BCBS. According to Mare (2019), risk is inherent to a bank's main operations. In support of these findings, Apostolik et al. (2009) provide examples of operational risk within a banking industry and highlight the following:

- Operational risk losses that may arise from internal and external fraud.
- Business disruptions by system failures.
- Failed internal processes.
- Inadequate staffing.
- Natural disasters and external forces such as pandemics.

According to Mare (2019), all bank endeavours involve operational risk. Therefore, it is critical to have a fundamental awareness of operational risk to identify potential controls for those risks, which serves as a basis for the following section.

1.4. Operational Risk in the Banking Industry

This section provides a summary of the operational risk within a banking industry to stress the consequences of effectively managing operational risk in banks.

According to the BCBS (2018), operational risk is defined as the risk of shortfall produced by insufficient or unsuccessful internal procedures, people, and systems, or external occurrences. Moosa (2007) describes operational risk as a series of hazards from the loss of critical employees, failed settlements, and noncompliance with theft, systems failure, and building destruction. Young (2014), on the other hand, describes operational risk as an organisation's exposure to possible deficits, causing business disruptions and unsuccessful execution of its functions. The IOR (2011) classifies operational risks into internal and external factors. Apostolik et al. (2009) demonstrate operational risks in terms of events. Jednak and

Jednak (2013) classify internal factors of operational risk into systems, people and processes and recognise external operational risk influences, including natural disasters and regulations.

Operational risk has become one of the most common risks faced by banks; therefore, supervisors and regulators in the banking industry have begun to stress the relevance of operational risk management (Moosa, 2007). According to Hefferman (2005), banks have begun to emphasise operational risk in addition to other risks they face. According to Helbok and Wagner (2006), to address operational risk in the banking sector, regulators, auditors and rating agencies opt to address operational risk separately from credit and market risk. As such, managing operational risk has become a priority for many banks within the banking industry (Young, 2012).

Commercial banks generally face various risks, including operational risk. However, the risks cannot be avoided; rather, banks must accept and manage the risks by ensuring that the effect of the risks is minimised. Hence, Saunders and Cornett (2008) emphasise the need to develop and implement appropriate risk controls and mitigations. However, an important question remains: can the identified risk controls and mitigations effectively protect the banking industry from global pandemics?

The banking industry plays a financial intermediation role by taking deposits and extending credit to viable ventures of personal, business, and corporate clients. To meet customers' needs, banks are persistently expanding and advancing their products and services (Central Bank of Lesotho Supervision Report, 2020). The banking industry strives to enable easy access to banking services through different platforms to customers through banking hall walks, digital platforms, internet banking and mobile services (Central Bank of Lesotho Supervision Report, 2020). The banking industry has improved through technological advancements such as digital access to banking services. Customers can transact through digital channels such as internet banking, digital wallets, and mobile banking services (Central Bank of Lesotho Annual Report, 2018). There has been a remarkable increase in the digitalisation of access to banking services and products, as reflected by the increasing number of users and transaction volumes of the internet and mobile channels (Central Bank of Lesotho Payment Systems and Settlement Reports, 2020). Customers are therefore enabled to transact through digital wallets, the internet, and mobile banking services when performing financial services (Central Bank of Lesotho Supervision Report, 2020). However, the BCBS (2020) indicates that the highly developed technology and advanced use of digital platforms expose the banking industry to operational risk. In Chapter 2, the operational risk and its factors are discussed in depth.

In recognition of the abovementioned developments within the banking industry, the management of banks highlights the significance of successful operational risk (BCBS, 2018). According to Young (2009), banks adopt BCBS recommendations to successfully manage operational risk, which highlights quantifying operational risk in the form of anticipated and unanticipated losses suffered by a bank. This approach provides a more purposeful method for operational risk management. The BCBS introduced Basel II in 2006, with the aim of encouraging banks to practice and prioritise effective risk management (BCBS, 2020). Understanding the Basel II concept is critical since it incorporates operational risk. The following section provides a brief description of the Basel II framework, as it is one of the supervisory risk management frameworks adopted by the banking industry.

1.4.1. Basel II

This section provides a concise description of Basel II, underlines the framework's purpose and intentions, and describes the fundamentals of successful operational risk management.

Basel I received several criticisms, which prompted the BCBS to introduce a revised framework to respond to the criticisms. The Basel Committee outlined a detailed capital adequacy to expand the scope of Basel I (Seliane & Sello, 2015). In 2004, the BCBS introduced a revised capital framework known as Basel II, which comprises three pillars, namely, regulatory capital requirements, supervisory oversight, and market discipline (BCBS, 2006). As stated by Seliane and Sello (2015), Pillar 1 is focused on establishing the minimum required regulatory capital for banks. Pillar 2 entails developing financial administration, which includes ensuring adequate capital valuation and completing regulatory examinations and assessments. Pillar 3 includes the market control for banks, including industrial training (Thejane, 2017).

Basel II was mostly intended to encourage a secure and sound banking system, inspire banks to implement risk management practices and balance competition between all regulated banks (BCBS, 2010). Furthermore, Basel II aimed to ensure that the international banking system remained stable. In addition, it is intended to create operational risk supervision for constricted risk control (BCBS, 2010). According to the BCBS (2018), the Basel II process of the risk management framework entails risk identification, risk assessment, risk measurement, risk analysis, risk monitoring and reporting, risk capital allocation and risk mitigation and control.

The BCBS (2020) highlights Basel II principles for effective operational risk control in banks, some of which are highlighted below.

- The bank's management should ensure that an adequate operational risk management culture is established throughout the organisation.
- Banks should formulate and execute an operational risk management framework that is integrated into the broader risk management process.
- A bank should have a clear governance structure with clear positions, and responsibilities should be clearly defined.
- The management of the bank should ensure that operational risk factors are understood by all employees to be able to identify and evaluate the risk factors.
- Management should ensure that banks develop processes for the effective analysis of operational risk.
- The bank needs to form and implement the monitoring process of operational risk exposures.
- Banks should have a strong oversight system capable of employing policies, processes and systems and adequate risk controls and mitigations.
- A business continuity plan should be established for banks to ensure the competence of continuing to operate during disruptions.

The BCBS (2020) further states that it is the responsibility of central banks to regularly evaluate the policies, processes and systems that are connected to the operational risk of banks. Thus, the areas that are explained by the principles of operational risk should be included in operational risk assessment (BCBS, 2020).

This section provides a brief overview of operational risk in the banking business; however, research will be conducted in subsequent chapters to identify operational risk factors to determine appropriate risk mitigations and controls.

1.5. Problem Statement

Based on the preceding discussion, it seems that banks need to carefully manage operational risk issues and have appropriate control measures in place to address risks, either internally or externally.

The Lesotho banking industry is critical to the economy and continues to be a key provider of financial services and products in Lesotho; therefore, it is crucial to effectively manage operational risks during normal circumstances and during crisis events such as the COVID-19 pandemic. The COVID-19 pandemic has impacted the world economy. As countries were under lockdown, mobility was restricted, firms were closed, jobs were lost, and interest rates plummeted. The Lesotho banking industry was also impacted by these constraints, which put pressure on banks' credit management, service delivery, technical expenses, sales, and revenue as interest rates plummeted. As a result, banks defined internal controls that they

consistently adhered to in order to maintain proactive risk controls during the pandemic. Although the banking industry in Lesotho remained stable and profitable in 2019, risks were largely manageable, with operational risk rated as one of the crucial risks (Central Bank of Lesotho, Supervision Report, 2020). Owing to the nature of its operations, the Lesotho banking industry is nevertheless vulnerable to financial and nonfinancial risks. As previously stated, commercial banks must prioritise operational risk management since they are inherently exposed to operational risk in all bank transactions and activities. Consequently, the intent of this research is to analyse banks' operational risk experiences during the COVID-19 pandemic to determine operational risk control measures that banks can adopt to prepare for potential future crisis events. As such, this study aims to answer the following research question: What risk control measures are most suited to safeguarding banks from operational risks during crisis events? The purpose of the study will be addressed next.

1.5.1 Purpose of the study

The purpose of this study is to determine operational risk control measures to prepare and safeguard banks from potential operational risk exposures during crisis events based on the experiences of the COVID-19 pandemic. The following research objectives are pertinent to the purpose of the study.

1.5.2 Objectives

The study will be directed by primary and additional secondary objectives.

1.5.2.1. Primary objective

The primary objective is to identify the effect of the COVID-19 pandemic on the operational risk faced by the Lesotho banking industry to determine preventative control measures. The primary objective will be supported by the subsequent secondary objectives.

1.5.2.2. Secondary objectives

- Conduct a literature review on operational risk to identify control measures for a bank during a crisis event.
- Review the main influences of the COVID-19 pandemic on operational risk and the underlying risk factors faced by banks in Lesotho to confirm appropriate control measures to protect banks from similar future events.
- Conduct a quantitative study of the identified control measures for operational risk to protect banks against crisis events and to verify the contemporary applicability of the identified controls. The findings of the empirical analysis will be used to confirm the conclusions and serve as a platform for recommendations to achieve the objectives of the study.

The subsequent section covers the methodology that will be employed for the empirical analysis of the research.

1.6. Research Methodology

Leedy and Ormrod (2010) define research as the scientific collection, assessment, and analysis of data to generate interest. The purpose of this literature review on the operational risks faced by the Lesotho banking industry is to identify relevant risk factors and effective operational risk control measures to protect banks from potential negative influences induced by large risk occurrences such as pandemics. The literature review aims to obtain information on the primary effects of the COVID-19 pandemic on the threats and risk factors faced by Lesotho's banking industry and to establish the current applicability of the recognised controls. A thorough description of the research methodology is included in chapter 4. The next sections provide a brief introduction in this regard.

1.6.1 Research paradigms

Creswell (2009) characterises research designs as strategies and procedures that cover conclusions encompassing general beliefs about comprehensive methods of collecting and analysing data to form a conclusion. The research design is influenced by the underlying philosophical paradigms summarised as positivism, pragmatism, constructivism, and interpretivism (Creswell, 2009). However, this study will focus on positivism, as assumptions about positivism apply to quantitative research. Positivism favours researchers who seek objectivity and rely on statistical analysis (Leedy & Ormrod, 2010). Furthermore, according to Phillip and Burbules (2009), positivism is also intended to moderate a broader set of views into smaller and separate variables that comprise a set of research problems. This study seeks to identify risk control measures available for Lesotho to use against potential crisis events.

1.6.2. Research approach and design

This study adopts a quantitative approach, which, according to Salkind (2019), is in line with the typical positivity view that there is a single reality that can measure reliability and validity using a scientific principle. The quantitative research approach involves quantifying and analysing variables to obtain results (Apuke, 2017). Creswell (2009) states that quantitative methods seem to be the best indicators of the results of a study that focuses on the elements that may influence the results that must be recognised or understood. The benefit of using a quantitative approach, among others, includes making generalisation possible using scientific methods for data collection and analysis (Salkind, 2019).

Creswell (2009) states that quantitative studies employ assumptions through deduction and establish a literature review at the initial phase of the investigation to validate a theory rather than construct it. The assumption will then serve as the basis of the study, organising the

research question and data collection technique. Against this background, a quantitative method is best suited to this research, as the literature is applicable to risk management; common risk operational risk factors faced by banks and what impact COVID-19 has had on those factors were examined to determine the empirical problem. Cooper and Schindler (2008) define good studies as consistent and reliable. They proposed that a research design be developed to attain the objective of the study. The appropriate design for this study is a descriptive nonexperimental survey research design. Descriptive research examines the situation as it is and can be used to identify the characteristics of variables or the degree to which variables exist in a specific context or situation (Salkind, 2019). The survey design will enable indirect observation via questionnaires.

1.6.3. Data collection

A literature review represents the most important step of the research process. As noted by Onwuegbuzie, Leech, and Collins (2012), a thorough and sophisticated literature review is the foundation and inspiration for substantial useful research. The authors identified benefits that can be derived from conducting a quality review of the literature, among which are identifying the strengths and weaknesses of the various research approaches that have been utilised, identifying contradictions and inconsistencies, and avoiding unintentional and unnecessary replication. According to Kumar (2011), the researcher should be able to benefit from the literature review in the following ways:

- The research approach should be improved, and the understanding and emphasis of the research problem should be emphasised.
- The researcher's expertise in the research topic should be improved.
- The researcher should be able to contextualise the research findings.

As a result, it is critical that the literature highlights recent material on the risk management of banks, different risk factors, and the effect of COVID-19 on the operational risks faced by banks.

In research, there are different methods used to collect data, including primary and secondary data (Ajayi, 2017). As explained by Ajayi (2017), gathering data can be accomplished through a primary or secondary source. A primary source is whereby the researcher is the first person to obtain that data, while secondary data apply to where the data are already collected and produced by others (Salkind, 2019). Primary sources include surveys, observations, questionnaires, experiments, and personal interviews (Ajayi, 2017). For this study, a questionnaire was used to collect primary data because to address the problem at hand. Primary data are always specific to the researcher's needs, more accurate, and more reliable (Ajayi, 2017). Ajayi (2017) state that primary data are collected directly from people who are

experiencing a problem or who are trying to solve it. The questionnaire used for this study was designed based on conclusions drawn from the literature and the research objectives of the study and consisted of close-ended questions.

1.6.4. Data analysis

The sample data will be statistically analysed using Microsoft Office Excel 2016 and the Statistical Package for Social Science (SPSS) (2016). The survey results are evaluated using descriptive statistics to confirm control measures for protecting banks from crisis events.

1.6.5. Data measurement

Cooper and Schindler (2008) state that the description of the criteria include reliability, validity, and stability. These features improve the research by recognising that the data collected by the research instruments are capable of being used to draw conclusions and make suggestions.

1.6.6. Validity and reliability

It is critical for other researchers to be able to replicate a study. According to Sürücü and Maslakci (2020), reliability is the degree to which repetition of a method would yield identical results at different times. Creswell (2014) defines validity as the ability to efficiently quantify the impact of an empirical idea and establish the degree to which that significance can be considered true.

To ensure validity and reliability, the study will consider content validity, and the questionnaire will ask relevant questions derived from the literature. A designed questionnaire will be submitted to research experts to ensure that there is an alignment between the questions that have been asked and the research objectives of the study. The questionnaire will therefore be tested for validity before the survey is launched, as recommended by De Villis (2011). Owing to the small population targeted, the questionnaire will be pretested by other experts in risk management. Because banks operate in different establishments and some use professionals, specialists, or external experts, estimating the number of participants may be challenging.

Reliability will be tested using the Cronbach's alpha coefficient. The Cronbach alpha coefficient is regarded as the most widely used method for estimating internal consistency and reliability (Amirrudin, Nasution & Supahar, 2021). The Cronbach's alpha coefficient describes the reliability of a sum of measurements, where measurements represent rates, occasions, alternative forms, or questionnaire test items (Bonett & Wright, 2015). The detailed outcomes of the validity and reliability tests are presented in Chapter 4.

1.6.7. Generalisation

The questionnaire used was based on a 5-point Likert scale. De Villis (2011) deem the Likert scale to be the most reliable and effective method for analysing the opinions of a population. The Likert scale aims to rate the level of importance of the control measures and criteria according to the respondents' knowledge and experience and to confirm the current applicability of the control measures within their respective organisations. Therefore, the scale reflects the following:

1. To no degree.
2. To a lesser degree.
3. To a moderate degree.
4. To a degree.
5. To a full degree.

1.6.8. Sampling and population

The population of the study will consist of the banks of the Lesotho banking industry. There are four commercial banks in Lesotho and one banking operation within the central bank of Lesotho (Central Bank of Lesotho Supervision Report, 2020). The survey will involve two commercial banks (the Nedbank and Lesotho Post Bank) and the Central Bank (banking operations). The Central Bank provides banking services such as deposits and withdrawals for the government and banks (Central Bank of Lesotho Annual Report, 2020). Hence, it forms part of the sample population.

Johnson and Khoshgoftaar (2020) state that data should be collected from a sample of the population because it would be impossible to distribute the questionnaire to all participants of the population. Moore, Neville and Murphy (2010) suggest a stratified sampling method. The population consists of five banks, one of which is the banking operation of the Central Bank of Lesotho. However, only three banks participated in this research (Nedbank, Lesotho Postbank and Central Bank). The target participants are the bank's officials, managers and executives who work directly with operational risk management within banks – business managers, risk managers, compliance managers, financial managers and internal auditors.

1.7. Ethical Clearance

The University of South Africa (UNISA) policy on research requires that ethical clearance be applied from the relevant department by the researcher before proceeding with the data gathering from external participants. The researcher obtained ethical clearance at the Department of Finance, Risk Management and Banking before proceeding with the empirical research.

Authors such as Kumar (2011) and Cooper and Schindler (2008) develop research principles to ensure that the research is conducted ethically. The following principles were followed in this research:

1.7.1 Informed consent

The human participants involved in the study were informed of the data expected from the study, the purpose, and the information that was needed. Each participant was required to voluntarily read and sign a consent form (Kumar, 2011).

1.7.2. Deception

Deception is the practice of intentionally deceiving participants, restricting information to generate or conceal factors. Information may be withheld from participants to obtain more accurate results or to safeguard confidential data (Cooper and Schilder, 2008). This type of activity was avoided in this investigation.

1.7.3. Privacy, confidentiality, and anonymity

The identity of the participants was hidden. The collected data were password protected to maintain control. Participants' privacy and confidentiality must be protected and respected (Salkind, 2019).

1.7.4. Coercion, incentives, and sensitive information

Participation in the study was voluntary, participants were not offered any incentives for participation, and the researcher considered the sensitivity of participants in the survey.

1.7.5. Permission

The gatekeeper letters were obtained from each bank as an authorisation to include the bank in the survey.

1.8. Limitations and Delimitations

The study is restricted to individuals who are actively engaged in risk management in Lesotho banks. These include business managers, risk managers, compliance managers, financial managers, and internal auditors. The analysis is limited to the effects of COVID-19 on operational risks faced by the Lesotho banking industry; other risk types that may influence a bank are not covered in this study. The study is limited to operational risk, as it is clear from the literature that banks should prioritise operational risk due to their ability to be present in all the bank's transactions and activities. Banks are sensitive to information sharing; therefore, the study could have limitations in terms of the availability of data secured by banks.

1.9. Structure of the Study

The following chapters comprise the study:

Chapter 1: This introductory chapter provides a background and a short summary of the literature, emphasising the current banking industry in Lesotho, coupled with the primary risks faced by banks. The problem statement, research objectives and research questions are set, and a brief description is provided of the research methodology, along with ethical considerations and limitations of the study.

Chapter 2: Literature review on operational risk. This chapter presents a general overview of the important literature on risk management. The study's objective is to identify operational risk control measures that will prepare and protect banks from potential operational risk exposures during crisis events. To accomplish this objective, the researcher will analyse risk management frameworks to discover the typical components of a risk management framework. Furthermore, to confirm operational risk factors, this chapter defines and reviews operational risk. A review of the identified operational risk factors will be conducted to identify potential risk control measures.

Chapter 3: Review of COVID-19 as a pandemic: This chapter addresses the COVID-19 pandemic and the underlying operational risk exposures to link with the identified risk controls identified from the literature.

Chapter 4: Research Design and Methodology. The focus of this study is the research design adopted, which provides additional specifics on the research methods used to collect the data and the numerical methods utilised to analyse the data.

Chapter 5: Analysis of Survey: This chapter provides an analysis and interpretation of the survey findings based on a descriptive and statistical analysis of the questionnaire responses about the importance of operational risk control methods and their present applicability in various banks.

Chapter 6: Conclusions and Recommendations: Based on the literature and empirical research, the chapter will conclude with a summary of the study, followed by the key results, recommendations, and scope for future possible research.

The following chapter will present an overview of the research on risk management and frameworks, which will be used as a platform for identifying relevant operational risk control measures.

CHAPTER 2: LITERATURE REVIEW ON OPERATIONAL RISK MANAGEMENT

2.1 Introduction

This chapter provides an overview of the relevant literature on operational risk to identify control measures to protect organisations against crisis events. It elaborates on the concept of an operational risk management framework. Further, it identifies the typical components of an operational risk management framework to serve as a platform for identifying relevant risk control measures. However, it is important to initiate a literature review with an acceptable definition of risk management to ensure a secure basis for the literature review.

2.2. Defining Risk Management

Various interpretations and perspectives on risk management are highlighted in Chapter 1. Kanchu and Kumar (2013) defined risk management as the application of a proactive strategy to plan, lead, organise and control the wide variety of risks that an organisation encounters in its daily and long-term functioning. According to Khan, Hussain and Mehmood (2016), risk management involves the identification of influencing factors that could have a negative impact on the cost and hinder the business from achieving the desired goals. According to the BCBS (2021), risk management encompasses identifying risks and measuring and assessing exposure to those risks. Risk management also includes monitoring, control and mitigation as well as reporting to senior management and the board of directors on an organisation's risk exposures.

In addition, Baker, Filbeck, Holzhauser, Saadi, and Christian-loan Tiu (2015) regarded risk management as a practice that ensures that investors' interests are protected by ensuring that the business maintains its profitability. According to Wall (2009), risk management can be defined as the evaluation of alternative courses of action to reduce risk potential. Oluwaseyi et al. (2016) stated that risk management involves setting an appropriate risk environment to protect organisations from adverse outcomes or risk exposures. Bahamid and Doh (2017) defined risk management as an organised and comprehensive method tailored towards organising, identifying, and responding to risk factors to achieve a goal. Ahmad, Muhammad and Narullia (2021) indicated that risk management is a systematic way of looking at areas of risk and determining how each should be treated. Therefore, risk management is a tool that aims to identify sources of risk and uncertainty, determine their impact, and develop appropriate management processes (Ahmad et al., 2021). According to Berg (2002), risk management is an activity that integrates the recognition of risk, risk assessment, developing strategies to manage risk, and mitigating risk using managerial resources.

Several definitions have been investigated, and based on the above definitions, there seems to be a common understanding of what risk management means and how to define it.

However, for this study, the definition set out by the BCBS was adopted, which explains that risk management encompasses identifying risks, measuring and assessing exposure to those risks and monitoring identified risk exposures to identify possible controls and mitigations.

According to the BCBS (2018), a sound risk management system must have the following features:

- an active board and senior management oversight;
- appropriate policies and procedures;
- the comprehensive and timely identification, measurement, mitigation, control, monitoring and reporting of risks;
- an appropriate management information system (MIS) at all business levels of the organisation; and
- a comprehensive set of internal controls.

To justify the importance of risk management in an organisation, Kanchu and Kumar (2013) highlighted that managing risk does not entail preventing the risk from occurring; rather, it entails identifying it, acquiring full knowledge, and understanding the risk to be able to measure and mitigate it. Furthermore, Kanchu and Kumar (2013) mentioned that, for an organisation to survive, it must be fully able to foresee and prepare for risk events rather than reacting to the event only after it has occurred; therefore, they emphasised the importance of risk control. ISO 31000 (2009) highlighted the benefits that come with effective risk management, such as improved corporate governance, financial reporting, and stakeholder trust. In addition, effective risk management raises awareness that there is a need to identify risks and identify opportunities and threats for organisations to treat them accordingly (ISO 31000, 2009).

Owing to the many unfortunate events and a series of fraud incidents, terrorist attacks, and the comprehensive economic crisis of 2008, Du Randt (2011) indicated that risk management has become an important component of organisations. Kimball (2023) indicated that the increase in interest in risk management could also be the result of repeated and reported failures concerning risk management implementation. According to Young (2012), the global financial crisis of 2008 resulted in enormous losses for some banks. Stead and Smallman (2014) singled out poor organisational culture as a main factor that contributed to the failures of various institutions. For instance, Stead and Smallman (2014) revealed that within the Johnson Matthey Bank (JMB), there was no sufficient financial direction, there was a poor internal audit and no credit committee, and most of the staff members were incompetent and inexperienced, which led to poor credit assessment and substandard record keeping. The case of Barings Bank showed a vague corporate structure, with confused reporting lines and poorly defined managerial roles, which led to a failure to control and separate operational

functions (Stead & Smallman, 2014). The non-performance of Nigerian banks from 1987–2011 was also attributed to poor enterprise risk management (Oluwasey et al., 2016). The trend toward poor risk management was also highlighted in a series of bank failures in Lesotho. For example, the Lesotho Building Finance Corporation (LBFC) experienced major management challenges in the late 1970s because of lending practices (Matlanyane & Harmse, 2002). As a result, in 1993, it amalgamated with the Government Development Bank, the then-Lesotho Bank. Despite the merger, Lesotho Bank was also liquidated in 2001 for poor management. Similar problems were reflected in the Agricultural Development Bank, which led to its closure in 1998 (Matlanyane & Harmse, 2002). Therefore, as stated by the BCBS (2021), risk management is important because it empowers organisations with the necessary tools to adequately identify and assess potential risks to evaluate and control them. According to the Central Bank of Lesotho Annual Report (2020), most banks are moving closer to a risk-based management approach not only to ensure proactive risk management but also to adhere to certain regulatory requirements related to governance and risk management.

The preceding discussion shows that poor risk management by banks can result in low profit margins, failure and/or total collapse. However, as stated by the BCBS, effective management of risks within the bank entails identifying, measuring and assessing, and monitoring the risks. Based on the above views, risk management entails the process of identifying, analysing, controlling, and monitoring risk exposures that may hinder a business' performance. In conclusion, it is important that organisations clearly define risk management and ensure that it is known and understood by all employees to guide what risk management is and what value it can have on an organisation. According to Young (2018), for effective risk management, an organisation must ensure an embedded risk management framework to provide guidance and support effective risk management. Therefore, the subsequent section reviews the risk management framework.

2.3. Risk Management Framework

In this section, the risk management framework is briefly defined to identify the typical elements that aid as a platform for this study.

Rouse (2010) defined a framework as an intellectual structure that supports or guides the process. Similarly, Alberts and Dorofee (2010) indicated that risk management frameworks could be used to guide how to manage all risk types. In addition, a risk management framework is a tool that stipulates specific and accepted best practices to regulate risk management and defines key activities that are required to manage risk. However, it does not specify how activities must be performed (Alberts & Dorofee, 2010). The European Investment Fund (2010) clearly states that a risk management framework is a set of processes, tools and

strategies for measuring and controlling risks. According to ISO 31000 (2009), a risk management framework manages the entire process of risk management and ensures that it is effectively incorporated within the organisation. As such, risk management is an active component of governance, strategy and planning, management, reporting processes, policies, values, and culture. ISO 31000 (2009) further noted that a risk management framework is the responsibility of the board. Therefore, according to the BCBS (2018), the board of directors must ensure that an organisation's risk management framework includes detailed policies that set specific prudential limits on its daily activities. According to Girling (2022), having a solid risk management framework prepares management for upcoming risks and therefore enables them to equip themselves with tools and contingency plans to respond swiftly when a risk event occurs. Similarly, Young (2018) noted that a risk management framework serves as a conceptual structure that consists of components to guide the board towards making adequate business decisions. For example, an enterprise risk management framework encompasses the following components: the internal environment; setting objectives; identifying risk events; and assessing risk, risk response, risk control, information and communication and monitoring (Lai, Shad, Khan, Shad, K. & Ali, 2010). The above views confirm that a risk management framework is a tool that guides management towards effective risk management in an organisation. Therefore, organisations should determine and maintain a risk management framework that develops and communicates policies, standard procedures and limits that define responsibilities and authority to control risk exposures that arise from the activities of organisations.

Numerous risk management frameworks have been developed over the years; for example, Mare (2019) highlighted the risk management association framework (RMA), the ISO 31000 risk management framework and the Committee of Sponsoring Organisations of the Treadway Commission (COSO). These risk management frameworks will be addressed next to identify the components of a risk management framework. The identified components, as per the accepted definition of this study, will therefore be discussed in detail with the intention of identifying possible control measures for the Lesotho banking industry. The next section addresses the COSO risk management framework.

2.3.1. COSO risk management framework

COSO is a voluntary private sector initiative that focuses on improving organisational performance and governance through effective enterprise risk management, internal controls and fraud prevention (COSO, 2012). The COSO risk management framework consists of five components that influence organisations to establish their mission, vision, and core values; develop their strategy; and formulate and implement objectives. The COSO risk management framework consists of the following components:

- Culture: According to COSO (2012), culture entails the establishment of operating cultures within an organisation and a clear definition of the desired culture understood by all employees. COSO (2012) further stated that a culture of risk management supports the achievement of an organisation's mission, vision, and strategic objective. In addition, Chapman (2011) noted that the important aspect of a risk management culture is to have an embedded definition of risk management approved by the board, which should be a component of the risk management policy.
- Governance: Governance entails acquiring skilled, experienced, and qualified employees (COSO, 2012). According to COSO (2012), there should be transparent, well-defined, and consistent lines of responsibility for effective risk management.
- Strategy and objective setting: An organisation needs to determine its objectives before identifying potential risk occurrences, which can influence the achievement of organisational goals. Enterprise risk management ensures that management executes a method to describe ideas and ensures that the objectives are aligned with the organisational mission. Furthermore, strategy and objective setting entail a well-defined organisational risk appetite, evaluating strategies and formulating an organisation's objectives.
- Performance: Identify the risks, which are assessed to establish their severity so that appropriate risk responses can be implemented (COSO, 2012).
- Risk assessment: Entails assessing the risk influence and the possibility that an organisation can proactively plan on how to mitigate or respond to identified risks.
- Information, communication, and reporting: Entails communicating risk information within the entire organisation. Identifying and communicating relevant information can assist employees in performing their tasks and responsibilities.
- Risk monitoring: Risk monitoring involves monitoring risk responses and adjusting where necessary. According to COSO (2012), the risk monitoring stage assists an organisation in measuring the success of its implemented risk control strategies to improve them where necessary.

As the COSO risk management framework was previously discussed, banks can effectively control risk management when they create a risk management culture that is understood by all employees, acquire adequate skills, and provide a clear allocation of responsibilities. Furthermore, a bank needs to identify possible risk incidents and analyse the impact and likelihood of determining appropriate risk mitigations and controls. Therefore, based on the review of the risk management framework by COSO, the typical main components of a risk management framework can be identified as a risk culture, risk strategy, governance and risk structures, and risk management process.

Another risk management framework was developed by ISO 31000 and will be discussed next.

2.3.2. ISO 31000 risk management framework

ISO 31000 is a risk management standard that was published in 2009 by the International Organisation for Standardisation (ISO). The framework developed by ISO 31000 intends to assist organisations in managing different types of risk through the integration of risk management into the entire management system and assisting different stakeholders, such as policy makers and risk managers (Gjerdrum & Peter, 2011). The ISO 31000 framework comprises the following components:

- **Mandate and Commitment:** Through this component, a framework emphasises the importance of commitment, adequate planning, and clear and appropriate distribution of resources. Instilling the culture of risk management at all levels of the organisation and ensuring that it aligns with the risk management policy of the organisation.
- **Designing the framework:** a simple structuring of information on the risks to effectively manage them. It includes understanding the external and internal environment of the organisation. Integrating risk management into organisational processes, internal and external communication, and reporting forms an important part of the design of a risk management framework. In addition, adequate resource allocation, ensuring that qualified and experienced staff with appropriate skills are hired, is also a component of a risk management framework.
- **Implementing risk management:** an organisation ought to employ the framework for managing risks. The execution of a risk management process also warrants effective risk control. To successfully implement the framework, the organisation should specify the timeframe for implementation and explain the implementation approach. Organisations should also adhere to regulations and legal requirements and safeguard against the fact that their objectives are in accordance with the results of the risk management process. In addition, ISO 31000 (2009) posited that constant communication with stakeholders ensures an effective risk management framework. Risk management processes must be implemented by means of a risk management disposition at all organisational levels that are relevant to the mandate. The identified components of the management process include establishing the context, risk assessment, risk treatment, monitoring and review, and recording the risk management process (ISO 31000, 2009). ISO 31000 (2009) indicated that a risk management framework manages the entire process of risk management and ensures that it is effectively incorporated within the organisation. Therefore, risk

management is an active component of governance, strategy and planning management, reporting processes, policies, values and culture.

Based on the above discussion on ISO 31000, it seems important for management to commit to effective risk management through adequate planning and clear allocation of resources and responsibilities and instilling a risk management culture at all levels of the organisation. In addition, the ISO 31000 risk management framework emphasises the importance of designing and implementing an appropriate risk management framework that will guide effective risk management as well as managing the process of risk management. ISO 31000 (2009) also opined that acquiring adequate resources, appropriately allocating acquired resources and providing a clear description of responsibilities are important parts of effective risk management. Furthermore, ISO 31000 highlights the importance of adequate risk management. Based on the above discussion, culture, governance structure, the risk management process and risk management strategy can be identified as components of a risk management framework. The next risk management framework to be discussed is the risk management association framework (RMA).

2.3.3. RMA risk management framework

The RMA is a nonprofit-making member-driven professionals' association that consists of 2600 institutional members. The main objective of RMA is to improve the use of sound risk principles in the financial industry (IOR, 2019).

According to the IOR (2011), the framework developed by the RMA highlights the following components:

- Strategy: This demonstrates the general attitude and conduct of risk management in relation to organisational plans, policy, and governance structure.
- Process: Process encompasses the procedures and decisions used to manage operational risk in everyday activities.
- Infrastructure: Infrastructure refers to recognising the resources employed during management, which includes data and systems.

Baker et al. (2015) noted an integrated risk management framework or the “three Ms” of risk analysis, which comprises the following components: (1) risk modelling, which involves identifying risk threats and exposures that organisations may be exposed to as well as possible control measures; (2) risk measuring, which refers to risk assessment and likelihood; and (3) risk management, which entails all the actions needed to mitigate risk.

Based on the discussion on the RMA framework, it seems important for an organisation to link its risk management strategy with its overall strategy and identify the process of effective risk

management. The risk management process entails risk identification, risk measuring and assessment to determine the appropriate risk controls required to mitigate the acknowledged risk exposures. Therefore, based on the reviews of the RMA framework, it is concluded that risk strategy, the risk management process and infrastructure are important components of a risk management framework.

2.3.4. Concluding remarks

Based on the findings, for effective risk management, an organisation needs to develop and implement a risk management framework that will provide guidance and support towards achieving the objective of effectively managing risks. The RMA emphasises the importance of aligning risk management with the organisation's overall strategy and having adequate tools to effectively manage the risk management process. The COSO and ISO 31000 risk management frameworks emphasise the need for organisations to acquire adequate skills, clearly allocate resources, and provide a clear description of roles and responsibilities as well as instil a risk management culture within the entire organisation to effectively manage risks. An organisation needs to develop a risk management framework that will assist in managing the entire risk management process by including policies that stipulate a bank's method for identifying, assessing, monitoring, and controlling risks. Therefore, for the purposes of this study, the following components of a risk management framework can be derived: risk culture, risk management strategy, risk governance structures, and risk management process.

A detailed review of these components will be performed next, as they provide a stand for recognising and adopting applicable risk mitigation and control measures for operational risk.

2.4. Components of an Operational Risk Management Framework

This section provides details on the components of an operational risk management framework, namely, risk culture, risk management strategy, risk governance structures, and the risk management process.

2.4.1. Risk culture

Young (2020) defined risk culture as the norms and traditions of the behaviour of individuals or groups within an organisation, which determine how they identify, understand, discuss, and act on the risks faced by an organisation. The BCBS (2018) referred to risk culture as a bank's norms, attitudes and behaviours related to risk awareness, risk taking, risk management and controls. Huy, Thach, Chuyen, Nhung, Tran and Tran. T.A. (2021) defined corporate culture as the set of values and beliefs, behaviours, perceptions and thinking methods that are common within an organisation. However, according to the Federal Reserve Bank of New York (2016), risk culture is also a tool that encourages employees to work in a manner that is in line with the stated values of the organisation. Roeschmann (2014) also referred to risk

culture as the product of organisational and group learning about what has happened or has not happened in the past. In addition, Roeschmann (2014) stated that risk culture is a good and effective concept with formal and informal features. As stated by the Financial Stability Board (FSB) (2014), a risk culture influences management decisions and channels employees' behaviour in their daily activities. Furthermore, Parker and Bradley (2000) stated that risk culture encompasses general awareness, attitudes, and employees' behaviour towards risk and how well it is managed. According to Carretta, Farina and Schwizer (2017), effective risk culture is an important tool for long-term value creation and financial stability. Nicolini, Gärling, Carlander and Hauff (2017) confirmed that risk culture could affect how banks' investors estimate reputational impact on the business. In addition, Nicolini et al. (2017) indicated that bank managers and regulators should concentrate on the risk culture of rules and policies; however, this practice must include the compliant behaviour of employees. According to Young (2018), a risk management culture should be embedded in an organisation and must include a definition of risk, principles for managing risk and the values of risk management to the organisation. Chapman (2011) stated that ensuring the effectiveness of risk management practices must be part of organisational culture. According to Young (2014), an adequate risk management culture must reflect the organisation's ethics, values and attitudes towards risk management. For this study and based on the abovementioned findings, a definition of a risk culture by the BCBS (2021) will be accepted, as it clearly states that a risk culture is a bank's norms, attitudes and behaviours that are related to risk-taking, risk management and risk controls.

In conclusion, having a strong organisational culture influences managers and channels employees towards effective risk management. Therefore, it is critical for an organisation to embed a risk management culture. The board of directors and senior management of the bank should create a culture in which effective risk management and employees need to be prioritised and understood.

The next component of a risk management framework is risk governance structures, which will be addressed next.

2.4.2 Risk governance structures

Risk governance structures, as an element of a risk management framework, entail acquiring skilled, experienced, and qualified employees (Prewett & Terry, 2018). To elaborate on the concept, Naciti, Casaroni and Pulejo (2021) defined corporate governance as the set of rules and organisational structures that results in adequate operations of the organisation. Girling (2022) stated that governance defines the responsibilities and roles of employees within an organisation. Similarly, the BCBS (2018) points out that an effective governance structure

entails a clear definition of roles and responsibilities. In addition, the internal governance structure refers to the functions and processes that are established to oversee and influence the actions of the management of firms. According to Chung and Zhu (2021), governance provides resources to facilitate strategic actions. Kaplan (2004) referred to governance as the way in which organisations make decisions regarding policy and strategy. According to the BCBS (2021), strong governance involves balancing corporate performance with an appropriate level of monitoring. According to the Economic Cooperation and Development (OECD), corporate governance involves a set of relationships between the management of the organisation, the board, shareholders, and other stakeholders. Governance also provides the structure through which the objective of the organisation is set and the means of attaining those objectives and determining monitoring tools (OECD, 2009). According to Ross and Crossan (2012), good governance goes beyond just the control of the organisation; instead, it also provides a way in which an organisation is supervised to achieve the desired goals. According to Blunden and Thirlwell (2013), good internal governance is key for organisations to ensure sound risk management. Andries, Capraru and Nistor (2018) argued that governance is an important determinant of a bank's performance. Andries et al. (2018) further stated that banks with sensible governance are more efficient at allocating their resources, while banks with poor governance are likely to be exposed to risks during crises. In addition, Young (2022) indicated that primary role players could adopt three lines of defence towards successful risk management. That is, they should work as a team to effectively manage their risk experiences. For further elaboration, Muhsyaf, Cahyaningtyas and Sasanti (2021) highlighted that the first line of defence entails proactive identification and implementation of responsive measures should the risk event occur. The second line of defence includes risk managers who will be responsible for developing and implementing risk management processes and procedures. The last line of defence involves internal audits, which monitor and ensure the effectiveness of control measures. Young (2022) emphasised the importance of all-role players, understanding their roles and responsibilities in the management of risk. Furthermore, Young stated that risk management is the responsibility of all different levels within the organisation and recognises the following key role that players play:

- Board of directors: The board of directors oversees and monitors risk management within the entire organisation (Prewett & Terry, 2018). According to Young (2009), the board is accountable for guaranteeing that the management prioritises risk management within the organisation. In addition, Young (2022) indicated that the board needs to be aware of the important risks that an organisation is exposed to and ensure that corrective measures are implemented.

- Risk management: Risk management involves coordinating all risk management information on a centralised basis to ensure that a centralised source of risk information is accessible to all role players.
- Business management: According to Young (2022), it is the responsibility of business managers to provide regular feedback to the board regarding the performance of the business. According to Epitimehin and Obafemi (2015), business management is the implementation level of risk management, whereby managers are responsible for recognising risks and managing risk in their specific business activities and implementing appropriate responses.
- Internal audit: An internal audit is the mechanism that organisations use to assess the status of internal controls. In addition, internal audits are responsible for monitoring the effectiveness of risk controls and ensuring that risk management systems and processes are adequate. Internal audits further ensure compliance by the organisation with regulatory guidelines and evaluate policies and procedures to ensure that they are relevant (Epitimehin & Obafemi, 2015).

According to the aforementioned discussion, governance structures entail acquiring adequate skills and resources. In addition, effective allocation of resources and clear allocation of roles and responsibilities contribute to effective management of the organisation. Therefore, it seems that a solid governance structure and appropriate risk management policies serve as a platform for effective risk management.

To conclude, an organisation's operational risk management framework should include a governance structure to confirm risk management roles and responsibilities. Key roles are critical for effective risk management. First, business management oversees the bank's operations, which include proactive risk detection and management within the accepted limits of an organisation's risk appetite. Second, risk management is responsible for developing and implementing risk management methods and providing a centralised risk reporting and control function. Third, an organisation must conduct an internal audit to confirm that the risk controls established are effective. The board of directors has the fourth responsibility for overseeing the overall risk management process.

The next section addresses a risk management strategy as a component of a risk management framework.

2.4.3 Risk management strategy

According to Louw and Venter (2013), strategy in a risk management framework entails setting up an inclusive manner and method for risk management concerning organisational objectives, policy and governance models. Furthermore, Louw and Venter (2013) noted that

strategy is concerned with the organisation and its environment. According to COSO (2009), strategy and objective setting influence the establishment of a mission, vision, core value, strategy development, business objective setting and implementation and performance. In addition, effective strategy implementation ensures value creation for all stakeholders and secures above-average earnings for organisations (Louw & Venter, 2013). However, organisations need to focus on risk management to construct and safeguard the worth of the business (Frigo & Anderson, 2011). Furthermore, organisations need to link strategy and risk management and identify and manage risk in a highly uncertain environment (Mare, 2019). Mare (2019) further indicated that a risk management strategy entails a structured approach towards the management of risks. According to Mu, Peng and Maclachlan (2009), a risk management strategy helps management understand, identify, manage, and reduce risks. According to Mu et al. (2009), an effective risk management strategy could improve organisations' performance. With an appropriate risk management strategy, an organisation can successfully introduce new products through adequate risk assessment and management and avoid project failure (Mu et al. 2009). Frigo and Anderson (2011) indicated that considering risks during strategy planning and execution allows organisations to identify potential areas of risk and proactively plan for effective risk controls. According to Louw and Venter (2013), typical strategic planning entails the following:

- Vision refers to defining the vision of the organisation to determine its future.
- Mission entails the alignment of an organisations' business functions to support the defined vision.
- The internal and external environment refers to the evaluation of internal and external factors that could influence the product, service or overall success of the organisation.
- Strategic goals and objectives entail the defining of strategic objectives that are aligned with the vision and mission of an organisation.

As indicated by the IOR (2016), a risk management strategy must be aligned with an overall organisation's strategy, objectives, policies, and processes. In addition, Young (2022) stated that there is an integration between strategic planning and risk management. Thus, for each traditional step of a strategic planning process, a corresponding risk activity occurs. Therefore, a risk-based business strategy should be implemented.

According to Prewett and Terry (2018), strategy and objective setting, as components of a risk management framework, address organisational objectives. Prewett and Terry (2018) also included principles such as analysing the business context, defining the risk appetite for the organisation, evaluating alternative strategies and formulating the objectives of the business as tools for addressing organisational objectives. According to Prewett and Terry (2018),

strategic objectives are high-level goals that are aligned with the organisation's mission, vision and strategic objectives. Young (2022) highlighted that when considering these strategic objectives, management identifies risks coupled with these strategic choices and studies the implications of recognising control measures. Young (2022) further indicated that strategic objectives will indicate the individual goals of various business functions and will serve as a guide towards effective management of the corresponding risks. Frigo and Anderson (2011) posited that managers must consider strategy in accordance with the risks to identify, evaluate, measure and control risks at a high level of an organisation. According to Harner (2010), developing and understanding the linkages between top risk exposures, key strategies and objectives can help both management and risk oversight identify where risks overlap within an individual strategy and where certain risks may affect multiple strategies.

Therefore, based on the aforementioned factors, it seems critical for an organisation to apply its risk management strategy in combination with its overall business strategy to guarantee that the business strategy and objectives are within the set limits of the organisation's risk appetite.

A risk management process forms an important component of the risk management framework and will be addressed in the following section.

2.4.4. Risk management process

This section provides additional details on the risk management process as part of a risk management framework. The intention is to identify possible risk control measures that banks can adopt, especially in times of crisis.

As stated by Valsamakis, Vivian, Du Toit and Young (2022), a risk management process offers a planned approach that assists organisations in effectively managing risks. ISO 31000 (2009) suggested that the process of risk management must start with a framework of guidelines and implementation steps. Tohidi (2011) stated that understanding the risk management process and the people who take part in managing the process should ensure that an organisation reaches its mission. Harvey (2012) outlined a risk management process as follows: identifying risk, evaluating and assessing risk, developing a risk management strategy, executing a risk management strategy, and monitoring the process. Kanchu and Kumar (2013) outlined a risk management process involving risk identification, risk evaluation, monitoring and control. Furthermore, ISO 31000 (2009) indicated that a risk management process is the function of risk management techniques and policies for the effective establishment of a background, risk identification, evaluation, analysis, monitoring, control, communication and consultation. The Hong Kong Institute of Bankers (2013) also divided the operational risk management process into the following:

- Outlining the capacity and objective of the programme.
- Identifying and assessing significant risks.
- Measuring and analysing risks.
- Mitigating and controlling risks through management activities.
- Monitoring risks through expected reporting to management.

Based on the above information, a risk management process entails a planned tactic to risk management that outlines actions to be followed to effectively manage the risks. The components of a risk management process can be identified as follows: risk identification, risk evaluation, risk control and mitigation, and risk monitoring. These components are illustrated in a diagram (Figure 2.1).

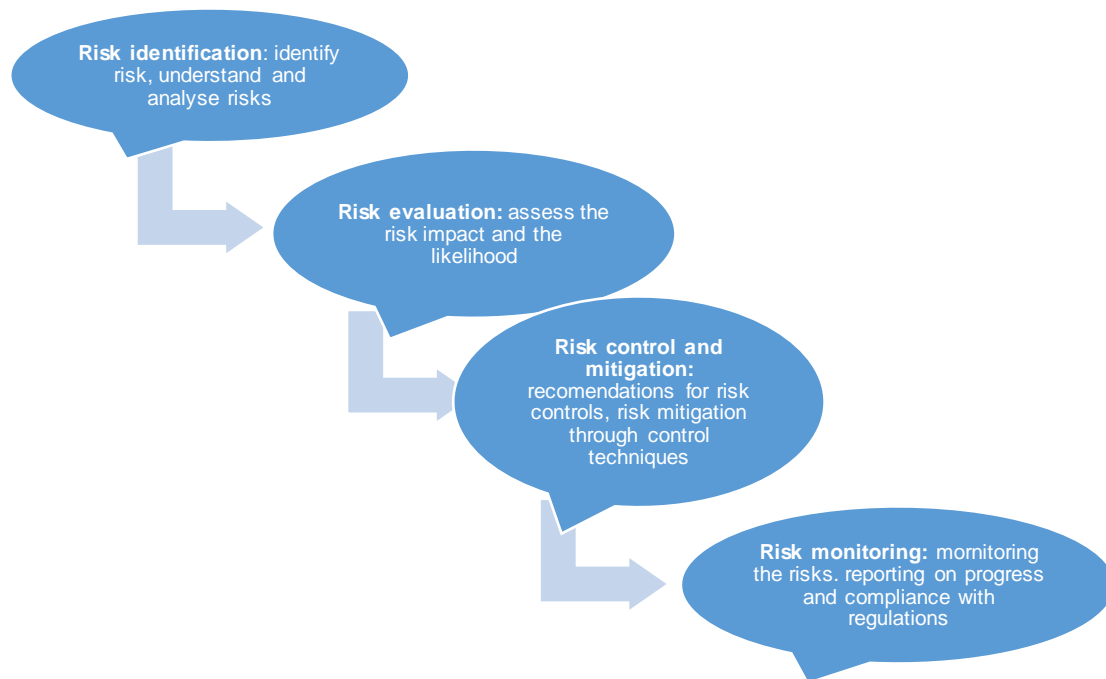


Figure 2.1: Components of a risk management process

Source: Adopted from Stanciu and Stanciu, V. (2010) and Kanchu and Kumar (2013).

The components of each risk management process, indicated in the figure, are described in the following sections.

2.4.4.1 Risk identification

Harvey (2012) referred to risk identification as the step at which an organisation identifies all the risks to which it is exposed and how those risks relate to a risk tolerance level. According to Young (2018), risk identification can be seen as an activity for identifying risk exposures that have the potential to affect the success and objectives of an organisation. According to Chapman (2011), identifying the sources of risk is the most crucial stage because sources are needed for proactive risk management; therefore, a better understanding of the sources will result in an improved risk assessment process and effective risk management. In addition, ISO 31000 (2009) stated that risk identification seeks to identify the risks that are applicable to organisations' strategic objectives. According to Chisasa and Young (2013), identifying risk exposure is the first step in a risk management process, and as Harvey (2012) stated, failure by an organisation to identify the risks that it is exposed to and failure to understand how risk exposure interrelates will result in decreased value. Berg, Bhatt, Kappelle, De Borst, Cramer, Der Graaf, Steg and Visseren (2017) suggested questions that may assist in the identification of risks as follows:

- Where, when, why and how are risks likely to occur?

- What specific risks are related to achieving each priority?
- What are the risks of not achieving those priorities?
- Who might be involved, for instance, in customers and investors?

Berg et al. (2017) noted that it is necessary to establish risk tools and techniques that can assist in identifying risks:

- Examples of possible risk resources.
- Scenario planning as a risk assessment tool.
- Process mapping.
- Documenting reports such as audit reports, programme evaluations, and research reports.

There are various methods that organisations can choose from to proactively identify risk exposures (Berg et al., 2017). According to Young (2022), it is important that an organisation decides on how to choose the method that is most suitable for the process. For example, workshops could be held if key participants were able to attend, while the use of a questionnaire would be more appropriate if participants could not attend physically. According to Khalilzadeh, Khalilzadeh and Zavadskas (2020), there are many ways in which banks can identify risks; however, they suggest that an organisation can improve its risk identification through SWOT analysis, which involves the examination of four factors, namely:

- Strengths, which refer to areas of the business that are more profitable.
- Weaknesses, which are areas of business that require improvement to increase profitability.
- Opportunities, areas that a business may explore to grow the business.
- Threats, which are risk areas of the business, must be minimised or eliminated.

According to Harvey (2012), brainstorming is one of the methods organisations can use to identify risks. Through brainstorming sessions, all employees are given an opportunity to explore ideas and share their views on possible risk exposures to the organisation. Once an organisation has decided on a choice of method for risk identification, the next step would be to customise the method to guarantee a coordinated tactic during the risk identification process. For example, Young (2022) suggested the following guidelines when a workshop has been chosen to identify the risks:

- Identifying areas of interest.
- Choosing suitable employees at the appropriate managerial levels to participate.
- Developing a format that can be used as guidance throughout the process.
- Appointing an expert to facilitate.

- Identifying the inherent risks to the business, as well as the procedures required to minimise or mitigate the risk's potential impact.

Kanchu and Kumar (2013) emphasised the importance of external stakeholders' engagement in risk identification. According to Kanchu and Kumar (2013), external stakeholders understand risk from an external perspective, affording an organisation important information on risk exposure to establish proactive responses. Harvey (2012) posited that for effective risk identification within an organisation, managers need to engage all employees at all levels and take note of customer complaints.

Furthermore, Young (2022) highlighted the following methods of risk identification:

- Questionnaires: Through this method, a gap analysis is conducted to identify the main risks that are inherent to certain activities within the organisation. Managers analyse the status of the activities to consider a solution to incomplete issues within the organisation.
- Risk checklist: through this method, management captures the lessons learned from previous experiences and evaluates whether the same risks still occur within the same organisation.
- Risk process flow analysis: This entails representing the processes of the organisation and determining the risks that the process is exposed to.

Based on the abovementioned findings, risk identification forms the first step of a risk management process. This approach entails identifying the risks that organisations may be exposed to proactively and implementing preventative controls. In conclusion, an organisation should choose an appropriate method to achieve its objective of effective risk identification.

According to Young (2009), to determine the suitability of control measures, the identified risks need to be evaluated. Therefore, the next section discusses risk evaluation.

2.4.4.2 Risk evaluation

According to Stanciu (2010), risk evaluation involves assessing the impact and establishing the likelihood of identified risks. Kanchu and Kumar (2013) concurred that identified risk exposures need to be analysed to determine the risk impact and establish the likelihood of risk exposure. Furthermore, Chapman (2011) referred to risk evaluation as the process that provides a concise perspective of the expected risk exposures or prospective possibilities coming from the organisation. According to Young (2014), risk evaluation entails the measurement and assessment of identified risk exposures. According to the above definitions, there seems to be a common understanding of risk evaluation, which involves risk measurement and assessment with the intention of confirming the risk impact and likelihood

of a risk incident occurring. According to Chapman (2011), managers should evaluate the risks to establish whether the risk is acceptable. Valsamakis et al. (2022) indicated that the purpose of the risk evaluation process is to determine the magnitude of various risks and their influence on profitability, capital, cash flow, or other important performance metrics. For instance, the reputation of an organisation. According to Harvey (2012), risk assessment should be performed every year or each time there is a material change in business strategy. Risk assessment is used to identify potential risk or threat; the output of risk assessment therefore helps individuals identify appropriate control measures to reduce risk to an acceptable level (Valsamakis et al., 2022). According to ISO 31000 (2009), management may then decide which risk to prioritise based on the risk assessment. Epetimehin and Obafemi (2015) indicated that there is a risk assessment process that needs to be followed to effectively manage risk.

According to Chapman (2011), for effective risk assessment, a risk assessment process must be followed, which involves analysing the identified risks to determine the potential likelihood and impact of the risk and determining control measures to mitigate the identified risks. In addition, Chapman (2011) states that after evaluating control measures, the rated risks that remain after attempts to minimise likelihood have been implemented (residual risks) are determined. According to Chapman (2011), a risk register is a document that records potential risks and possible mitigations and is updated to reflect the rated risks in terms of probability as an outcome of the risk assessment. The updated risk register, indicating the high-level residual risks, can then be used to define the key risk indicators, which can be escalated to responsible persons to manage (Chapman, 2011).

Risk can also be evaluated through a decision tree. This approach entails representing decision options and outcomes in a consecutive manner to consider uncertain outcomes. Decision tree analysis helps to manage risk to help select the best strategy where there is uncertainty. Young (2022) further indicated that risk evaluation could be qualitative, which is a statistical form of risk calculation in which the analysis of risk exposures is presented in terms of rating scales to determine the chances of the risk event occurring as well as the impact it might have on an organisation. According to Anton and Nucu (2020), a qualitative risk assessment often offers support for further investigation of a quantitative assessment; however, it can also provide the information needed for risk management. According to Young (2022), risk self-assessment is one of the most common qualitative methods of risk assessment. Anton and Nucu (2020) indicated that the risk self-assessment approach allows each business unit to assess the risks to which the unit is exposed. However, this approach still requires assistance from central operational risk control. Additionally, risk may be evaluated through a quantitative risk assessment. A quantitative risk assessment determines

the possible influence of risk on an organisation based on the numerical quantity of risk (Young, 2022).

According to the above, it seems clear that risk evaluation entails analysing identified risks to determine the likelihood of the exposure and the possible impact of the risk. The output of the risk evaluation will therefore help to identify appropriate risk controls to avoid the risk or reduce it to an acceptable level. Furthermore, various methods are available for risk evaluation. However, Young (2022) indicated the significant use of data from qualitative and quantitative approaches to effectively evaluate the identified risks. As a result, organisations should have processes in place to analyse the identified risks, and the analysis of the identified risks should include both qualitative and quantitative data for a successful review.

After evaluating the identified risks, the results can be used as inputs for effective control measures. The next section addresses risk mitigation and control.

2.4.4.3 Risk control and mitigation

Risk control and mitigation were identified in the previous sections as components of the risk management process and constitute an important part of this study because the main objective of this study was to determine appropriate risk control measures before and during crisis events.

Olson and Wu (2008) described risk control as the activity of measuring and implementing controls to lessen or avoid the impact of risk elements. Epetimehin and Obafemi (2015) associated risk control with implementing control measures to minimise the outcome of risk occurrence. Young (2014), on the other hand, indicated that risk controls involve the application of techniques to reduce the probability of loss. According to Kanchu and Kumar (2013), risk control and mitigation entail recommendations for risk controls, mitigating the risks through control techniques and delegating relevant personnel to address the risk. According to Young (2014), the use of control techniques will reduce the likelihood of a risk event occurring. However, Olson and Wu (2008) stated that risk control and mitigation could be reactive, which means implementing risk control measures after risk has occurred. Risk controls can also be proactive, which indicates allocating resources to mitigate the risk before it occurs. In addition, Epetimehin and Obafemi (2015) stated that risk is inherent in the operations of an organisation. Therefore, organisations must implement appropriate risk controls and mitigating techniques to lessen the effect of the risk, should the event occur. According to the BCBS (2010), a bank must have an adequate control system that includes procedures, policies, proper internal controls, and risk mitigation and distribution techniques. Young (2022) suggested three types of risk controls to reduce operational risk. First, according to Blunden Thirwell (2013), preventative controls are implemented to prevent a loss from

occurring. Second, detective control measures ensure that a loss event is identified to implement appropriate preventative controls to prevent an incident from reoccurring. According to Blunden and Thirwell (2013), detective control measures address the effects of the event. Third, contingency controls are procedures that are required to ensure that an organisation or a business area remains viable after a risky event has occurred (Blunden & Thirwell, 2013). For example, an appropriate disaster recovery site could be used by an organisation in case of a disaster.

Young (2022) stated the following categories of risk control decisions:

- Accepting the risk: The bank accepts the outcome of a risk occurrence because the losses are of such a character that they are accepted and ignored (Vanem, 2012). According to ISO 31000 (2009), risk may be retained by an informed decision, accepting the burden of loss from a particular risk. Kesharwani and Tripathy (2012) concurred and indicated that banks may retain high-frequency risks but have a low impact and therefore accept the possibility of certain losses. Possible tools for accepting risk include daily control standards and checklists.
- Mitigating or reducing risk: This refers to an approach in which a bank needs to create and implement control procedures that decrease or avoid losses. According to Harvey (2012), since risk is inherent in the banking industry, strategies to reduce the likelihood or impact of risk exposure should be developed. For example, ISO 31000 (2009) suggested removing the source of the risk and mitigating the risk by completely removing the threat. Possible tools include specific risk control measures, internal audit assurance and business continuity plans.
- Avoiding risk means avoiding a business choice that could result in unacceptable losses and have an unfavourable effect on the bank. When a bank decides to avoid risk, it has decided that it is not able to incur a loss that has a high probability of occurrence, and if this is realised, it has the potential to ruin the strategic objective of the bank (Dermine, 2013). According to ISO 31000 (2009), a bank may decide not to go ahead with the activity that increases risk exposure. Thus, risk is managed by adjusting the original approach of the project with the intention of eliminating the events that threaten the business.
- Transferring the risk: According to Young (2022), risk transfer does not entail transferring the actual risk of the organisation to the third party. Rather, the actual risk exposure remains with the organisation, while the effect of the risk is shared with the third party, which is willing to share a loss at a stipulated budget. For example, a bank can choose to shift the effect of a risk to another party, such as by outsourcing the

project or using contracts to shift specified liabilities to a third party. Risk transfer also occurs through the purchase of an insurance policy through which the effect of a risk is passed from a policyholder to the insurer (Hakenes & Schnabel, 2010). According to Harvey (2012), risk transfer includes buying business interruption insurance to handle unplanned expenses incurred due to events such as cyberattacks.

Young (2009), on the other hand, suggested that pillars of risk controls are necessary to ensure an effective risk control process, and they are discussed below:

- Policies and procedures: This entails establishing a risk management policy to ensure a consistent approach towards effective risk management across the entire organisation. The policy statement should specify how risk management will be approached and provide overall roles and responsibilities. The policies require approval from the board and need to be consistently updated to ensure a positive contribution to an organisation.
- Internal controls: entails developing and implementing internal controls to ensure effective management of the identified risks.
- Roles and responsibilities: This entails having an organisational structure that supports risk management, acquiring appropriate skills and ensuring proper allocation of those skills.
- Risk reporting: Through adequate reporting of risks and the provision of accurate data in risk reports to appropriate personnel, timely decisions to mitigate and control the risks will be made. Internal risk reporting can be accomplished through an organisation's management information systems, as well as external risk reporting to regulators and shareholders.

It seems evident that the control component of a risk management process is critical either to prevent a loss from occurring or to minimise the effect should a loss incident occur. Additionally, having appropriate tools, techniques and resources is crucial for effective risk management control and mitigation. Therefore, organisations need to determine and implement appropriate preventative risk control measures to protect them from potential risks such as pandemics.

According to Young (2022), there are two important control methods for operational risk, namely, information security and business continuity management. According to Harvey (2012), information security means that for an organisation to be able to control operational risk, it must set up a suitable processing technology and information security. Information security is the possibility of loss or other damage that an organisation could suffer because of

a breach of confidentiality, unreliable information, or the unavailability of timely information (Harvey, 2012). Due to an increase in digital ways of doing business, it is important to have data protection backup as well as disaster management recovery sites in case of disruptions (Arduini & Morabito, 2010). Some risks may entail an organisation changing its operating site; therefore, it is important to ensure adequate security controls against cyber threats to ensure that the organisation's information is not manipulated (Craigien, Diakun-Thibault, & Purse, 2014).

A detailed discussion on cyber threats and securities will be covered in the upcoming sections. Another crucial factor is information management, defined by Craigien et al. (2014) as the protection of information from unwanted misuse. To effectively manage information security, organisations should have information security policies to ensure the confidentiality, availability, and integrity of information within the organisation. Arduini and Morabito (2010) also shared the view that to lessen the impact of technology risk, organisations must have technology disaster recovery plans and develop physical security and data protection policies. In addition, organisations should establish an information security culture by motivating staff through training and using internal controls to obey security principles such as trust adhering to privacy principles and risk management (Arduini & Morabito, 2010).

According to Young (2022), another important operational risk control method is business continuity management. According to Arduini and Morabito (2010), organisations need to develop a business continuity management plan (BCMP) or framework, which clearly states how operations will be maintained in the event of an interruption that could cause damage or loss for an organisation. According to ISO 31000 (2009), business continuity management (BCM) is a set of complete processes that assist organisations in identifying potential threats that can affect an organisation. This approach entails effective responses that intend to secure the interests of the organisation's stakeholders. ISACA (2010) indicated that BCM is the management process that identifies potential threats to an organisation and the impact on business operations that those threats, if realised, might cause. The BCM provides a framework for building organisational resilience with the ability to effectively respond to ensure that stakeholders' interests, business reputation and organisational brand are protected (ISACA, 2010). Furthermore, Svata and Fleischmann (2011) defined BCM as the development of strategies, plans and actions to provide an alternative for operating critical processes of an organisation. According to Young (2022), the BCM should include the following factors:

- The business continuity plan (BCP), which, according to Svata and Fleischmann (2011), refers to documented procedures that guide organisations to respond, recover, resume, and restore to a predefined level of operation following or during

a disruption. It focuses on developing plans and procedures necessary for enabling successful contingency planning. According to Zawada (2014), a business continuity plan should be able to address the following objectives:

- Identify the major risks of business interruptions. To achieve this objective, the business must identify critical functions that must be performed to remain operational and profitable. Potential risk exposures must be identified and analysed so that the business can conclude whether to mitigate, absorb or avoid the risks (ISACA, 2005).
- Train employees and test the plan to ensure that it was effective. To achieve this objective, training and test methodologies should be developed, and adequate training of disaster recovery teams must be provided. This approach ensures that the BCP is adequate for addressing the identified risks and establishing if all team members understand their roles as well as reducing panic and building confidence among the disaster recovery team members (ISACA, 2011).

According to Arduini and Morabito (2010), business continuity must include the following components:

- People: refers to the recovery of employees and physical workspaces.
- Processes: refers to developing a strategy to locate, test and execute a plan.
- Technology refers to the recovery of data contained in a disaster recovery plan. Having a clear business continuity plan helps to protect an organisation against interruptions to the system.
- Contingency planning: Develop a plan to mitigate or reduce the impact of the identified risk. An important component that assists in mitigating or reducing the impact of external risks is the development of a disaster contingency recovery plan, which outlines procedures that must be followed when a disruption occurs. According to ISACA (2011), a disaster recovery plan comprises consistent actions to be undertaken prior to, during and after a disaster. A sound disaster recovery plan is developed from a comprehensive planning process involving all the enterprise business processes. Disaster recovery strategies include the use of alternate sites, redundant data centres, reciprocal agreements, telecommunication links, disaster insurance, business impact analyses and legal liabilities (ISACA, 2010).
- Emergency management, which entails ensuring that there is a process that an organisation must introduce to address an event that could disrupt the business. An organisation should perform drills to ensure that it is prepared for when an event

occurs. According to Boin and Hart (2010), the quality of communication and collaboration across emergency services are important factors for effective emergency management.

- Disaster management refers to disaster management. Disaster management outlines steps necessary to address and mitigate the effect of a negative event, often while the event is still occurring. For example, earthquakes, floods, and fires. According to Young (2022), disaster management entails the involvement of all stakeholders who could be affected by the disruption so that they can also proactively plan or prepare if a disaster occurs. Young (2022) emphasises the importance of engaging all parties that may be affected by the disaster to ensure that they understand the disaster and plan accordingly. The planning should involve all essential services, such as medical departments, fire departments and security departments.

Epetimehin and Obafemi (2015) further emphasised the importance of organisations having business continuity plans to continue operating even during disruptions. According to Arduini and Morabito (2010), business continuity planning helps residents maintain their economic activity in disaster areas by enabling them to continue operating during and after the disaster. With a proper business continuity plan, banks may still be able to take advantage of profit opportunities and earn customer trust while still providing a healthy and safe working environment for their employees.

Based on the above discussion, risk controls and mitigations entail having appropriate techniques and tools to proactively or reactively respond to the identified risks. Thus, an organisation should have alternative or backup facilities to assist in maintaining its operations during or after a crisis event. BCM is an imperative element of effective risk control for unforeseen risk exposures, such as the COVID-19 pandemic. Hence, having an appropriate BCP serves as a guide for reactive and proactive mitigation and control of unforeseen external risk factors. For that reason, important aspects of an effective BCP include data protection, information management, disaster recovery sites, disaster recovery teams and well-detailed disaster contingency recovery plans, which outline how the plan would be executed.

According to Young (2020), risk mitigation and control are dynamic processes that require continuous monitoring to determine whether implemented controls are appropriate. Therefore, the next section addresses risk monitoring.

2.4.4.4 Risk monitoring

An additional important component of a risk management process that has been identified is risk monitoring. According to Young (2014), risk monitoring aims to monitor the identified risks as well as the effectiveness of the implemented control measures against those risks. Young

(2009) referred to risk monitoring as the operational process whereby an organisation ensures that it complies with organisational policies and procedures and ensures the effectiveness of risk management activities. Chapman (2011) concurred with Young (2009), stating that risk monitoring is aimed at monitoring the performance of risk responses and advising on the need for proactive risk management interventions. As stated by Berg et al. (2017), risk management is dynamic and therefore requires regular monitoring. ISO 31000 (2009) suggested that organisations should have appropriate suitable reporting mechanisms at all levels within them to support proactive management of risks. Risk monitoring entails risk supervision, reporting progress and following up on the level of compliance with regulatory requirements (Kanchu & Kumar, 2013). It involves regular checking and surveillance and therefore forms part of the risk management process (ISO 31000, 2009).

Based on the above discussion, risk monitoring should entail monitoring the effectiveness of the implemented risk responses, reporting to, and advising relevant risk officers about any changes. The risk-monitoring task is usually delegated to the chief risk officer or risk manager and further to team members. ISO 31000 (2009) indicated that the board must plan the monitoring of risk to ensure that control measures against identified risk remain effective. In addition, Young (2015) stated that risk monitoring should also be performed regularly, as the continuous monitoring of risks will certify that counteractive activities against risk exposures are engaged. Therefore, according to Berg et al. (2017), risk monitoring must first entail a description of how outcomes of risk treatment will be measured. Second, risk monitoring validates that the risk management process and the documentation are still valid. Third, risk monitoring considers the current regulatory environment and industry practices, which could have changed during the intervention period. In addition, the BCBS (2021) indicated that it is critical for organisations to keep records of risk monitoring and must provide a report to both internal and external stakeholders.

According to Chapman (2011), an adequate monitoring step should have the following features:

- display an alert or notification;
- ensure that opportunities and risk are determined when monitoring the internal and external context;
- implement timely responses to opportunities and risks;
- continuously update the risk register on the changing circumstances; and
- provide a progress report.

Furthermore, Rostami (2016) indicated that risk monitoring could be performed using the following tools and techniques:

- Reassessing the risk: regular review and reassessment of the risk register to determine or evaluate the risk status.
- Auditing the risk: engaging qualified auditors in risk audits ensures systematic and timely risk monitoring and risk responses.
- Performance analysis: through a performance analysis, an organisation reviews the project's milestones to ensure that no risk has been disregarded. Performance analysis allows rapid responses to changes and new risks.
- Stakeholders' meeting: engaging with all relevant stakeholders to review risk data and update risk management strategies as needed.

Based on the preceding discussion, the conclusion is that monitoring is a component of a risk management process that entails monitoring the effectiveness of risk responses. Therefore, it seems important that banks regularly supervise the risks across the organisation to ensure that the risk control approaches remain relevant. Regular monitoring will provide information on risk status and assist management in improving mitigation strategies where necessary. In conclusion, an organisation should have monitoring instruments in place, such as an audit, to ensure that stated policies and procedures are followed and that all operational risk processes are effective.

2.4.4.5 Summary of conclusions of a risk management framework

Based on the above discussion, effective risk management entails having an appropriate risk management framework that will assist an organisation in addressing risk management challenges and serve as a guide throughout the risk management process. The risk management framework ensures that the process of risk management is effectively incorporated within the organisation. According to the COSO, ISO 31000, ORMF and RMA frameworks, the common components of a risk management framework can be classified as risk culture, governance structures, risk management strategies, and a risk management process. It is further evident that for effective risk management, an organisation should embed a strong risk management culture within the entire organisation that will influence managers' decisions and channel employees' behaviours towards effective risk management. The board of directors and management need to create a culture that practices effective risk management control. Furthermore, it seems that solid corporate governance and appropriate risk management policies serve as platforms for effective risk management. Therefore, an organisation needs to acquire adequate skills and clearly allocate roles and responsibilities in terms of identifying threats and assessing the likelihood and impact of threats to determine appropriate risk mitigation and control measures. Regarding a risk management strategy, it can be concluded that aligning a risk management strategy with an organisation's business strategy could serve as a basis for effective risk management. An organisation should develop

a strategy and set objectives to assist management in identifying and analysing the risk impact and likelihood of perceiving appropriate controls or mitigations. Furthermore, it seems that a risk management process forms an important component of a risk management framework and entails identification, evaluation, controls and mitigations, and monitoring. The discussion emphasised the need for organisations to identify risk exposures and to be proactive in developing appropriate responses. However, an organisation needs to evaluate the identified risks to develop and implement suitable controls. Appropriate preventative risk control measures need to be determined and implemented to protect organisations from potential risks such as pandemics. Business continuity management and information security management have been identified as primary operational risk control measures. An appropriate BCP serves as a guide for reactive and proactive mitigation and control of external risk factors such as COVID-19. However, for a BCP to be effective, it should entail data protection, information management, disaster recovery sites, disaster recovery teams and detailed disaster contingency recovery plans, which outline how the plan would be executed. Furthermore, it is important to monitor the identified risk and the effectiveness of the implemented control measures.

Operational risks are fundamentally present in all organisational operations and activities (Mare, 2019). Therefore, the next section focuses on operational risk with the intention of elaborating on the risk factors to which banks could be exposed to determine appropriate control measures.

2.5. Operational Risk

The significance of managing operational risk within the banking industry is emphasised in chapter one. In addition to what was dealt with regarding operational risk in Section 1.4, this Section aims to elaborate on additional definitions of operational risk to identify the underlying risk factors. These operational risk factors will be used as a platform for a literature review in terms of potential control measures that an organisation can implement to proactively manage operational risks during a disastrous event such as a pandemic.

2.5.1 Operational risk definition

Various authors have identified different definitions and views of operational risk. For the purposes of this study, identifying a suitable definition that clearly reflects the underlying operational risk factors is important and will assist in determining relevant control measures in a structured way.

According to Young (2014), operational risk refers to the risk that an organisation may incur losses because of failed processes and systems, internal failures, and external forces. Girling (2022) described operational risk as the possibility of an organisation failing due to the inefficiency of people, technology, processes, external influences and customer relationships.

Kulpa and Magdon (2012) further defined operational risk as the risk connected with the loss because of system and process failures, inadequate control, improper management, or human error. Yang, Hsu, Sarker and Lee (2017) adopted the definition of the BCBS, which states that operational risk is the loss resulting from inadequate or failed internal processes, people, systems, and external events. This definition also includes legal risk, although it excludes strategic and reputational risk. Coleman (2011) inferred that losing a business opportunity while systems are down, settling a wrongful dismissal claim, being penalised for late filing of documents, employee theft and missing customer records are hazards of daily running of the business and are referred to as operational risks. Most of these definitions refer to factors such as people, processes, systems (technology) and external threats, which can be seen as the underlying operational risk factors. In addition, as indicated in Chapter 1, Section 1.4, it seems that most organisations in the financial industry adopted the definition by the BCBS (2018); therefore, this definition will also be applicable for this study.

According to Epetimehin and Obafemi (2015), operational risk is inherent in all financial products, activities, processes, and systems, thus emphasising the importance of effective operational risk management in financial institutions. The BCBS (2021) mentioned that operational risk needs to be understood by all employees, and it is important that organisations develop a risk management framework that clearly communicates the concept of operational risk and underlying risk factors so that the risk can be managed. Therefore, it can be concluded that organisations need to have a clear understanding of the definition of operational risk and ensure that the adopted definition displays operational risk factors (processes, people, systems and external factors), which should enhance the management of the risks in a structured way. As such, it seems important that an organisation should ensure that all employees understand the definition of operational risk and the relevant risk factors to identify the risk and determine appropriate operational risk control measures. Therefore, the next sections will focus on operational risk factors to identify potential risk control measures that are specifically applicable for crisis events.

2.5.2. Process risk

Moosa (2007) mentioned that ineffectiveness or inefficiencies in the number of business processes inside the firm are examples of process risk. These include value-driven processes such as developing products and support for clients, as well as value-supporting processes such as human resources, information technology, and operations. According to Blunden and Thirlwell (2013), operational risk factors include payment or settlement failure, documentation that is not fit for purpose, errors in valuation pricing models and processes, project management failure, and internal or external reporting (mis) selling. Apostolik et al. (2009) described process risk as potential losses that are related to a business process. According

to Young (2022), process risk is the risk that business processes are not sufficient, resulting in an unexpected loss. Young (2022) identified the following variables as potentially contributing to process risk:

- Processing a new product and services.
- Business processes.
- Control processes.
- Process of starting a new business.

Various authors have indicated numerous incidents of corporate collapses and scandals because of poor operational risk management. Hendrikse and Hefer-Hendrikse (2012) stated that missing deadlines, power failure and communication breakdown can interrupt a bank's operations and lead to financial losses. Yasuo Hamaka, a copper trader at Sumitomo Corporation in Japan, neglected to declare losses for almost three years in 1996 because part of the copper market he controlled on his own, resulting in a financial loss of (US \$) 2.6 billion (Hendrikse and Hefer-Hendrikse, 2012). In 2002, Arthur Anderson of WorldCom in the United States was able to hide expenses worth \$3.9 billion due to misconduct and insubstantial internal controls; as a result, shareholders lost \$100 billion, and 17 000 jobs were lost (Jednak & Jednak, 2013). The above examples can be the result of inadequate internal controls, such as reporting processes and audits; continuous examination and monitoring; and inadequate segregation of duties (Blunden and Blunden, 2013). According to Isoh and Nchang (2020), data entry errors, collateral management failures, incomplete legal documentation, unauthorised access given to client accounts, and vendor disputes are examples of process risk events that may result in substantial losses for banks. Additionally, Jednak and Jednak (2013) indicated that inaccurate information or information that falls outside the corresponding accounting period could seriously affect accounting records.

Based on the above discussion, process risk is a loss of revenue or failure to meet business objectives due to inefficient or ineffective processes. Organisations need to develop policies and procedures to maintain a consistent approach towards effective risk management within a bank. Internal controls will further assist banks in preventing errors and indiscretions, identifying problems and ensuring that appropriate responses are carried out. Finally, risk reporting, which entails adequate reporting of risks and the provision of adequate data to responsible parties, ensures that timely decision-making regarding risk mitigation is obtained. To protect organisations and ensure that they remain operational during a crisis event, a business continuity management tool should be developed.

In conclusion, banks need to develop adequate policies and procedures to safeguard and manage operations in times of crisis. Additionally, banks should develop a BCM tool to

safeguard and manage risk during a pandemic. The following section covers people as operational risk factors.

2.5.3. People risk

According to Blunden and Thirlwell (2013), people risk includes fraud, breaches of employment law, unauthorised activity, lack or loss of key personnel, inadequate training and inadequate supervision. Human error by an employee or internal or external fraud may have a negative impact on organisations and can be seen as a risk to people (Apostolik et al., 2009). Moosa (2007) referred to employee absence, inadequate employee training and recruitment as people risks. According to Hendrikse and Hefer-Hendrikse (2012), in 2001, HIH insurance was also exposed to operational risk because of poor management and strategic decisions. Poor strategic decision-making can be the result of many factors, such as time constraints, poor judgement, office dynamics, incomplete information and excessive optimism (Hendrikse & Hefer-Hendrikse, 2012). Saunders and Cornett (2008) posited that poor judgement could occur when employees make decisions that do not add value to the growth of the organisation. Several organisations were also affected by people risk in South Africa, for example, accounting fraud and mismanagement by the Regal Treasury in 2005; accounting fraud and mismanagement by Fidentia in 2009; and failed management by Leisurenet in 2006 (Jednak & Jednak, 2013). According to Saunders and Cornett (2008), human error can occur due to a variety of factors, such as fatigue, stress, or distraction; panic; and malicious intent. Therefore, Jednak and Jednak (2013) emphasised the importance of employees' wellbeing. A malicious intent act occurs when employees deliberately engage in an action that is harmful to the organisation and in turn results in financial losses. Jednak and Jednak (2013) highlighted that failure of operational (people) risk management can be due to inadequate cross-training of employees, non-standardised processes and procedures, poor quality control measures, inadequate background checks on new recruits, or lack of skills. According to Saunders and Tossey (2013), these efforts include loss prevention through training, development, and employee wellbeing. Furthermore, it is critical to perform a thorough background check on new workers joining an organisation to establish their criminal history and community status (Arduini and Morabito, 2010). According to the BCBS (2010), appropriate segregation of duties is an important control that prevents responsibility conflict and protects an organisation against internal fraud.

Based on the preceding background information, intentional behaviour, such as fraud or malicious damage; errors, such as mistakes caused by fatigue or incompetence; lack of management supervision; and inadequate staffing levels, are risk events that could be caused by people employed by an organisation. It is important for an organisation to employ employees with relevant skills and clearly allocate roles and responsibilities. In addition, it is

important for an organisation to identify and include employees who are responsible for carrying out critical internal processes that must always be operational in its BCP. In addition, employees who have been tasked with carrying out these critical functions need to be trained to instil confidence and avoid panic during a crisis and establish safe working conditions for employees to ensure their welfare.

2.5.4. System risk

According to Apostolik et al. (2009), system risk refers to computer system, technology and system failures. The BCBS (2020) described system risk as system collapse and business distractions. Network failures, viruses in banking information systems, connectivity issues, software and hardware (data) failures, and electronic banking failures are just a few examples. Young (2014) added that system downtime could also result in the loss of business due to new deals, which could not be captured and processed on time. According to Blunden and Thirlwell (2013), system risk encompasses failures throughout the development and implementation stages, as well as insufficient resources. In addition, Moosa (2007) stated that system/technology failure, system integrity and system suitability are system risk exposures caused by breakdowns and poor project management. Yazdi and Kabir (2018) noted the following threats to system risk:

- Physical threats – resulting from physical access or damage to IT resources such as servers. These could include theft, damage from fire or floods, or unauthorised access to confidential data.
- Electronic threats – A hacker could obtain access to organisations' websites, resulting in IT systems being infected by computer viruses with an intention to compromise organisations' information.
- Technical failures – unintentional errors in technology-based systems, typically leading to the undesired disruption of normal operations.
- Infrastructure failures – loss of internet connection, therefore interrupting the business operations in the process.

Svata and Fleischmann (2011) stated that information systems and/or information technology risk assessment address data/information processing. Therefore, by managing IS/IT risk, an organisation could reduce the likelihood of "low quality" information. Furthermore, effective management of IS/IT increases resilience to cyber-attacks through increased awareness of potential threats and the implementation of control measures to reduce the likelihood of cyber-attacks. Ugwuja, Ekunwe and Henri-Ukoha (2020) noted that the world has resorted to digital banking, which exposes banks to technology risks such as cyber threats; according to Wang, Nnaji and Jung (2020), such banking is a malicious act intended to steal or damage data. The threat of cybersecurity attacks poses a great challenge for internet banking. Therefore, banks

should take responsibility for ensuring a more secure internet-banking environment for their customers (Ugwuja et al., 2020). Kesharwani, Sarkar and Oberoi (2019) indicated that banks are also responsible for creating awareness among their employees and customers of the cyber-security risks and frauds that can cause them to become victims. For example:

- Phishing: This is used to entice victims to give away their password or information willingly. According to Ankale, Adesina and Akarah (2016), phishing has become one of the most common threats affecting the financial sector. Through phishing, customers are sent emails from a fake website with the intention of encouraging them to disclose personal information, such as usernames and passwords, to log into their accounts so that the criminals can access the customers' bank accounts without their knowledge to defraud them (Hassan, Lass & Makinde, 2012). According to Ankale et al. (2016), phishing takes advantage of customers who are not familiar with the exact web addresses and interfaces of a bank.
- Hacking: Another cyber threat identified within the financial industry (Olasanmi, 2010). According to Olasanmi (2010), criminals design programmes used to monitor the movement within an organisation's network. The activity of hacking identifies weaknesses in a computer system or network to exploit security so that hackers can access customers' personal data. Unauthorised access to an organisation's computer systems affords hackers an opportunity to steal, change or destroy information. Through this programme, important customer information is collected, therefore violating customers' information privacy.

Arduini and Morabito (2010) indicate that an organisation must identify threats to digital banking, assess the potential impact of such threats and develop ways to secure systems. In this regard, Alghazo, Kazmi and Latif (2017) proposed an approach that incorporates more responsibility to banks to ensure that customers adhere to information technology policies, such as the following:

- Enforcing the regular changing of passwords.
- Enforcing complex passwords.
- Enforcing users to use virtual keyboards by disabling keyboard login.
- Enforcing sending an SMS notification/email if a login was detected from an untrusted device.
- Enforcing the sending of SMS tips for a safe internet banking experience.
- Enforcing security practices by using machine-based learning to detect any unusual behaviour of internet-banking users.

According to Kesharwani et al. (2019), it is critical for a business to hire expert cybersecurity professionals and create a cybersecurity framework that would act as a monitoring tool.

Furthermore, a bank ought to have a BCP in place to protect itself during crisis events, which will cover the procedures and provisions for the successful continuation of business operations.

Arduini and Morabito (2010) indicated that technology is another important aspect that must be included in the BCP. Therefore, the BCP must indicate how an organisation will be protected from technological interruptions. Furthermore, Arduini and Morabito (2010) state that organisations must develop physical security and data protection policies. Based on the above discussion, as well as the discussion in Section 2.4.4.3 on controls and mitigations, the expanding use of online platforms within the banking industry gradually exposes banks to technology or system risks. Hence, there is a need for banks to identify possible threats to developing proactive control measures.

The following approaches seem important for the effective management of system risk:

- Development of information data protection policies.
- Development of data backup facilities.
- Development of a cybersecurity framework.
- Having an alternative disaster recovery site.

In conclusion, the literature reveals that the banking industry is exposed to several system risks, such as data and information breaches as well as cyberattacks. It is further evident that the use of technology by banks has increased, therefore exposing banks to more system risk. Therefore, banks need to include system risk in their risk management strategy to determine appropriate responses. It is the responsibility of a bank to ensure a more secure digital banking environment for its customers and to create awareness of cybersecurity for both employees and customers. Banks need to develop a cyber-security policy and have a contingency plan that outlines procedures that must be followed for effective management of system risk during a crisis event.

Crisis events are usually likely to disrupt operations; therefore, it is important to anticipate external risks such as pandemics to proactively control and mitigate those risks.

The next section discusses external risk as an operational risk factor with the intention of identifying suitable control measures.

2.5.5. External factors

Moosa (2007) defined external risks as the risks that occur due to the influence of issues such as regulatory changes, competitor behaviour and external fraud. Blunden and Thirlwell (2012) included outsourcing (and insourcing risk), natural and other disasters, political risk and utility failures as examples of external risk. According to Heffernan (2005), external risks are events

that have a negative impact and are beyond the organisation's control. According to Moosa (2007), examples of external risk factors include criminal activities, natural disasters, changes in government legislation and economic changes.

Based on the definitions and perspectives presented above, as well as the context of COVID-19 in Chapter 1, COVID-19 serves as an example of an external risk factor. As indicated by Mare (2019), an external risk can comprise, among other things, a criminal activity that can be unpredictable, have a negative impact, be beyond an organisation's control and disrupt business operations, which can lead to financial loss. In addition, external risk factors are unpredictable risk factors that are beyond an organisation's control and can influence the performance or operation of its business. As indicated by Young (2022), because external risks are unanticipated and unforeseen, it might be difficult for an organisation to manage them proactively. However, for effective control of external risks during a disaster, a bank needs to develop a detailed business continuity plan as a risk control measure to ensure its ability to operate even in the event of severe external disruption. To ensure business continuity, organisations must adopt strategies, rules, standards, and procedures to govern the management, implementation, and control of people, processes, and systems connected to contingency plans (Young, 2022).

Based on the aforementioned results, it can be emphasised that the BCM is an important risk control measure for external risks. Therefore, for banks to be able to operate during or after a disaster has occurred, they should develop a BCM policy, which should include the following (also refer to Section 2.4.4.3):

- Disaster management entails the engagement of all concerned stakeholders so that all parties are proactively prepared for a disaster.
- Business continuity management aims to establish the likely impact of a disaster to minimise the impact of risk.
- A bank needs to identify potential incidents, assess the likelihood of incidents, and prepare a business continuity plan. The BCP must be adequately defined and indicate roles and responsibilities during and after the incident so that all stake holders understand what must be done to continue with the operations, should the disaster occur.
- Emergency management is the process initiated to address an incident that could disrupt the business and threaten the safety of employees.
- A bank needs to have a crisis management plan that is specific to disasters or pandemics.

- A bank should proactively plan to establish processes, procedures and back-up sights that will continue to operate despite the impact of the disaster or the pandemic.

While external risk factors are unpredictable and outside of an organisation's control, organisations should have a documented business continuity strategy in place to ensure business continuity during or after crises.

2.6. Summary of Operational Risk

Operational risk is recognised as one of the key exposures that banks are confronted with; therefore, it is critical that employees have a comprehensive awareness of operational risk, particularly for the board, senior management, and functional departments. Employees will be able to identify operational risk exposures and choose relevant risk controls and mitigations if they understand the view of operational risk.

The literature has revealed processes, people, systems and external events as the main factors of operational risk. The literature reveals that it is important for an organisation to have measures in place to mitigate the abovementioned risk factors.

Risk can be attributed to intentional behaviours such as fraud or malicious damage; errors such as mistakes caused by fatigue; incompetence; lack of management supervision; or inadequate staffing. Furthermore, failed processes and ineffective or inefficiencies in business are examples of process risk. Nonetheless, the increased use of online platforms exposes banks to technology or systems risk, such as cyberattacks and information or data breaches. Banks are also vulnerable to external risk factors that are unpredictable and beyond the control of the organisation.

2.7. Conclusion

This chapter provides a literature overview of operational risk management with the aim of identifying control measures that can be implemented to serve as proactive measures against potential disastrous events. The literature reveals that it is important to establish an acceptable definition for risk management, and an organisation should embed a risk management framework. A risk management framework aims to act as a model for effective risk management and communicates policies, standard procedures and limits that define responsibilities and authority to control risk exposures that arise from the activities of an organisation. The typical components of a risk management framework were determined to be the following:

- Risk culture. A risk culture ensures the embedding of the norms, attitudes, and behaviours of an organisation's employees related to risk-taking, risk management, and risk controls. As such, ensuring that an organisation has an embedded risk

management culture in place is crucial. Employees should prioritise and understand the significance of risk management.

- Risk management strategy. An organisation needs to align its risk management strategy with the overall business strategy to ensure that the business strategy and objectives are within the set limits of the risk appetite of an organisation.
- Governance structures. An organisation should ensure that its governance structures are incorporated into its operational risk framework to confirm its roles and responsibilities. The key role-players in risk management were confirmed as follows:
 - Board of directors. The board is responsible for establishing a risk management culture, performing an oversight function in terms of risk management and approving risk management policies.
 - Business management. The management is responsible for identifying and managing the risks for their units within the parameters of an approved risk appetite.
 - Risk management. This role player is responsible for setting risk management policies and providing a centralised risk reporting and control function.
 - Internal audit. This role player is responsible for providing an independent view of the effectiveness of risk policies and controls.
- Risk management process. The following four steps of the risk management process were determined:
 - Risk identification. Entails identifying and understanding the inherent risks faced by an organisation.
 - Risk evaluation. Concerns the assessing of the identified risks in terms of potential impact and likelihood of the risks.
 - Risk control and mitigation. Involves the establishing of risk control and mitigation measures for the identified risks.
 - Risk monitoring. Entails the continuous monitoring of the risks and control measures and reporting on any inadequacies.

The literature review revealed a suitable definition for operational risk as the risk of a loss resulting from inadequate or failed internal processes, people, systems, and external events. An analysis of this definition indicated that the underlying risk factors for operational risk are the following:

- People risk.
- Process risk.
- System/technology risk.

- External events.

For each underlying operational risk factor, control measures were identified that could be necessary to protect an organisation against potential disastrous events. These control measures are as follows:

- People risk
 - Organisations should employ employees who will carry out the identified critical functions during times of serious events.
 - Employees should be trained to ensure that they understand what needs to be done during times of crisis.
 - Organisations should ensure employees' health and safety during times of crisis events such as a pandemic.
- Process risk
 - Organisations should develop adequate policies and procedures to safeguard and manage operations in times of crisis.
 - Organisations should develop a BCM policy to protect them from disastrous events.
- System risk
 - Organisations should develop a cyber-security policy to safeguard organisations against system risk.
 - Organisations should include a contingency plan, which must outline the procedures that must be followed to effectively manage disruptions of operational systems during a crisis.
- External risk
 - Organisations should develop business continuity management (BCM) and information data protection policies.
 - The BCM should include disaster risk management, which entails the involvement of all stakeholders responsible for managing the risk event.
 - The BCM should indicate through emergency management how the business continuity plan (BCP) will be executed during a disaster event.
 - Organisations should perform regular emergency drills to test whether planned risk controls are effective.
 - All employees should be adequately trained in cybersecurity management.
 - Organisations should protect themselves against unauthorised access to the organisation's data and ensure the development of information data protection policies and data backup facilities.

- Organisations should have an alternative disaster recovery site that can be accessed during a disaster to ensure the continuation of operations.
- Organisations should identify critical activities that must remain functional during a disaster to ensure that the organisation remains operational.

Although the abovementioned controls are not exhaustive, the identified control measures could serve as a platform for organisations to be proactive in protecting themselves against potential disastrous events such as the COVID-19 pandemic. The next chapter will address the COVID-19 pandemic as a case study for the Lesotho banking industry to identify practical concerns and possible links with the identified operational risk control measures, which could support the aim of this study.

CHAPTER 3: IMPACT OF COVID-19 ON OPERATIONAL RISK FACTORS

3.1. Introduction

This chapter examines the COVID-19 pandemic to identify operational risk exposures for each underlying risk factor, namely, process risk, people risk, system risk, and external risk factors. Based on the conclusions drawn in Chapter 2, the identified risk factors will be linked to appropriate control measures, which may form the basis for the Lesotho banking industry to be proactive in preparing for future pandemics and crisis events, which could have a negative effect on the business operations of a bank. Therefore, the next section will focus on how people risk is affected by the COVID-19 pandemic.

3.2. People Risk

Based on the discussion in section 2.5.3, people risk includes workplace safety, staff absenteeism, and significant employee loss due to death, insufficient training, internal fraud, and theft. To mitigate the effects of the COVID-19 pandemic, governments have implemented strategies based on social distancing, national quarantine and the shutdown of nonessential businesses (PWC, 2021). However, because of the critical role of the banking sector, banks had to remain operational, although they were still required to comply with the implemented control policies implemented to address the pandemic. Nonessential functions of the bank, such as periodic payments and project reports (progress reporting on the banks' ongoing projects), were performed from home to comply with restrictions such as social distancing, while other employees responsible for the critical operations of the bank remained onsite. Examples of these critical operations include accepting customers' deposits, withdrawals, clearing of cheques, chequebook collection, and teller services (Ashraf & Goodell, 2022). As such, it is apparent that banks employ and train employees who are responsible for the critical operations of the bank during a crisis event. Furthermore, PWC (2021) stated that the banking sector's essential nature requires some employees to operate onsite despite restrictions and exposes them to the effects of the pandemic, which leads banks to provide necessary safety equipment for protection against the pandemic.

According to Ramasamy (2020), the COVID-19 pandemic not only affects employees' physical health but also affects their psychological well-being. In this regard, Usman, Cheng, Gul, and Shah (2023) stated that uncertainty during the pandemic was likely to make individuals doubtful about the profitability and future of the company, which added to the uncertainties surrounding their employment, possibly adding to mental health. According to Sarwar, Abdullah, Imran and Fatima (2023), employees' anxieties about their health also contribute to emotional weariness, which negatively affects their performance. According to Sarwar et al. (2023), these uncertainties negatively influence employees' psychological empowerment, resulting in reduced innovative behaviour and well-being. Therefore, it seems crucial that

banks safeguard employees' health and safety during a crisis to ensure their continuous well-being. In addition, Usman et al. (2023) demonstrated that the COVID-19 pandemic disrupted regular workplace practices and that banks were forced to change and adjust their working environment to a flexible working system that requires employees to work in virtual or online environments. As a result, employees became confused about their roles and responsibilities during the pandemic; hence, it seems essential that banks continually train their employees to ensure that they understand what they are supposed to do during a crisis.

To conclude, the above discussion revealed that banking services are essential and need to remain operational during crises; therefore, banks need to identify employees who will carry out the critical functions of the bank during a crisis event onsite or virtually. Banks need to provide continuous training to employees to ensure that they are prepared to fulfil their roles and responsibilities during a crisis. In addition, a bank needs to provide emergency health and safety facilities to ensure that employees remain safe and healthy throughout a crisis. The next section reviews the exposure to process risk during the pandemic.

3.3. Process Risk

It was concluded in Section 2.5.2 that process risk entails inadequate processes or procedures that could result in a loss. Because of the COVID-19 pandemic, banks had to adjust and change their working environment. According to the PWC (2021), adjustments, such as allowing employees to work remotely, affect banks' internal processes. Kaka (2021), for example, stated that COVID-19 had an impact on financial statement preparation, audit engagement, and reporting. Therefore, it became essential for a bank to ensure that its policies and procedures are in place to manage operations in times of crisis. According to Korzeb and Niedziółka (2020), these changes and adjustments further impact banks' planning procedures. They also have an impact on crucial internal control processes (Kaka, 2021). According to PWC (2021), almost every transaction in the bank is accountable for internal controls. This emphasises the importance of internal controls for the operations of a bank. However, the COVID-19 pandemic and consequent remote work have made it difficult for banks to implement and control processes, such as the segregation of duties and limited access to records for reconciliations, which could expose banks to additional risks (Tamásné Vőneki, 2020). As such, it became apparent that the bank's processes, policies and procedures remained effective during a crisis. According to COSO (2009), clear policies and processes reduce risk while maintaining effectiveness; therefore, it is imperative that policies and procedures include how a bank's crucial services will be maintained during normal times and a crisis. In addition, Tamásné Vőneki (2020) highlighted the impact of the COVID-19 pandemic on banks' communication procedures. According to Tamásné Vőneki (2020), communication was critical since the pandemic caused unusual workplace settings, such as

working remotely. As a result, banks need to change their communication strategies to maintain stable information flow among employees and maintain relationships with customers. For example, banks had to collect essential contact information and build positive relationships with the media (Tamásné Vőneki, 2020). It is thus apparent that banks need to develop a BCM policy, which should include communication strategies during crises. In addition, a defined BCM policy should detail the planning processes to ensure that banks continue to offer acceptable services and maintain critical bank services during a crisis. As indicated in Section 2.4.4.3, communication is an important factor that should be included in a bank's business continuity plan to enable clear and effective communication flows during a crisis. Therefore, it is essential that a bank include clear communication processes among internal and external stakeholders in its BCP to avoid possible disruptions of a bank's operations and maintain an appropriate flow of information.

In conclusion, for banks to be prepared for a crisis event, it is essential to develop adequate policies and procedures to ensure the continued operation of business processes. The policies and procedures should also stipulate effective communication strategies between all stakeholders to ensure the flow of essential business information for continued business operations. This can be achieved by a BCM policy, which should entail the detailed business continuity planning process that addresses a crisis.

3.4. Systems Risk

System risk refers to computer systems, technology, and system failure, which can disrupt business processes. (BCBS, 2010). During the COVID-19 pandemic, technology and digital services advanced within the banking sector due to limited physical services available (PWC, 2021). For example, the Central Bank of the Lesotho Annual Report (2020) claimed that due to countries' lockdowns, banks increasingly adopted digital financial services to ensure and maintain convenience and efficiency. According to Hundal and Zinakova (2021), the COVID-19 pandemic had an impact on the banking industry's use of financial technology, which exposed institutions to cyberattacks. For instance, bank fraud in Nigeria has evolved from low-tech fraud to computer infections to cyberattacks (Wang & Envilov 2020). The lack of sophisticated technologies available to prevent cyberattacks and the low level of legislative compliance appear to be the factors that have reduced cybersecurity capacity (Wang et al., 2020). Lallie, Shepherd, Nurse, Erola, Epiphaniou, Maple and Bellekens (2021) concurred by stating that following the COVID-19 pandemic, cyberattacks became more prevalent, with 3 to 4 unique cyberattacks on banks reported each day.

According to Ramasamy (2020), banks were forced to maintain engagement with their customers and to communicate through mobile devices. In this regard, cyber criminals could

send customers SMS messages or emails with the intent of controlling their bank accounts or credit cards for unauthorised use. For example, according to Plachkinova (2021), cyberattacks in the European Union increased during the COVID-19 pandemic, whereby attackers followed victims online using the COVID-19 pandemic to their advantage by devising phishing campaigns. As a result, technology adoption in the banking sector has increased, which has increased banks' exposure to cyber threats and data breaches. Therefore, it has become crucial for banks to develop cyber-security policies that clearly indicate how both internal and external stakeholders access digital banking and practice responsible security. A cybersecurity policy aims to describe general security expectations and the roles and responsibilities of the bank. Furthermore, the North Carolina Banking Institution (2021) reported that as more institutions, including banks, embrace digitisation to survive the increasingly digital world, customers in possession of banks become more vulnerable to cyberattacks. Hence, there is a need for banks to upgrade their cybersecurity measures. In addition, the increasing shift to digital banking has exposed banks to data breaches. For example, the Bank of America suffered a data breach on April 22, 2020, resulting in unauthorised access to customer data (North Carolina Banking Institution, 2021). Therefore, banks need to develop data protection policies to protect themselves against unauthorised access to data. Plachkinova (2021) supports this by stating that improving data privacy legislation will increase consumer trust in banks, safeguard customers from data injury, and reduce the financial impact that a bank may suffer after a breach.

In addition, governments introduced measures such as total lockdowns to mitigate the impact and spread of the COVID-19 pandemic. Thus, to comply with these measures, banks had to remotely perform nonessential functions. Banks were compelled to modify their systems to assure integrity even when conducting off-site work (Gonda & Tarazi, 2022). Therefore, it is essential for banks to develop a contingency plan that outlines procedures that will be followed to effectively manage operational systems during a crisis event. It is also essential that a bank develop data backup facilities to avoid the loss of important data. Owing to increased technology and digitisation within banks and the implementation of remote working because of COVID-19, it is essential for banks to have alternative disaster recovery sites (DR sites). A DR site can be accessed during a crisis to ensure that the bank's system operations remain functional during a crisis, thus maintaining the bank's integrity.

In conclusion, to safeguard a bank against system risk, it is essential to develop an adequate cybersecurity policy, which should include a process to ensure data and information security. In addition, it is crucial to establish a continuous communication process to inform all stakeholders of cyber activities or threats to ensure proactive control measures and contingency plans to manage system risks.

The next section focuses on the COVID-19 pandemic as an external operational risk factor linked with appropriate risk controls, as identified from the literature.

3.5. External Risks

External risks include factors that are beyond a bank's control and are unexpected (Young, 2022). In Chapter 2, it was concluded that external risk is the risk that may develop because of external obstacles. The COVID-19 pandemic is an example of an external risk factor. The pandemic had a detrimental influence on the economy, was beyond the control of organisations and was unexpected (WHO, 2020). Attempts to contain the pandemic affected the financial industry and its activities (Ashraf & Goodell 2022). Banks' techniques, operational norms, and infrastructures had to change (Bitar & Tarazi, 2022). As Young (2022) stated, external factors are unpredictable yet demand proactive management. Although countries were under lockdown during the COVID-19 pandemic, banks were considered an essential sector that had to remain operational during the pandemic (PWC, 2021). Therefore, banks had to identify critical functions of the banks that had to remain operational. They had to prioritise available resources toward the identified critical activities to ensure that banks remained operational during the pandemic. In compliance with government restrictions to control the spread of the COVID-19 pandemic, such as social distancing, some activities had to be performed remotely, while others remained onsite (PWC, 2021). Therefore, having a documented BCM would assist banks in ensuring business continuity during a crisis event. The BCM should include internal and external stakeholders of the bank who are responsible for business continuity. According to PWC (2021), new working environments, such as remote working and working with few employees, are needed to comply with social distancing. Employees became confused about their roles and responsibilities. Therefore, it was important for banks to have a defined business continuity plan to assist them in outlining the process of dealing with the crisis event and ensuring that all stakeholders understood their roles and responsibilities. However, the business continuity plan needed to be tested to ensure that all employees understood their roles during a crisis and to ensure its effectiveness.

In conclusion, to safeguard a bank against external factors during a crisis, it is crucial to have a BCM process, which includes the participation of all stakeholders responsible for business continuity. A BCM should include the process of dealing with a crisis event that could disrupt the business or threaten the safety of employees. Additionally, a BCM should include a defined BCP to ensure that all stakeholders understand their roles and responsibilities during a crisis event. However, it is crucial to perform drills to test the effectiveness of such a plan. The BCP should also stipulate which functions can be performed remotely during a crisis event.

3.5. Conclusion

This chapter provides some indications of banks' operational risk experiences due to the COVID-19 pandemic and actions taken to align these decisions with the operational risk control measures identified in Chapter 2. These actions were linked and discussed in terms of the control measures indicated in Chapter 2 for each underlying risk factor. According to the literature, the underlying operational risk factors are people, processes, systems, and external events. According to the literature, people risk includes workplace safety, employee absenteeism, the loss of key personnel because of death, inadequate training, internal fraud, and theft, whereas process risk refers to failing processes and procedures that result in a loss. According to the literature, system risk consists of a loss to the bank because of failed systems, while external factors include natural disasters and pandemics. According to the literature, to prepare for crisis events, banks should have trained employees who will efficiently continue to perform their essential activities. Furthermore, banks should identify critical functions that must remain operational during a crisis. According to the review, the BCM is an important tool for protecting banks during a crisis. Nonetheless, the review also revealed the increasing rate of digital banking and the expanding adoption of technology used by the banking industry, which exposed the industry to system risks.

Based on the discussion on operational risk in Chapter 2 and the COVID-19 pandemic in terms of people, processes, systems and external risk factors, the following conclusions regarding operational risk control measures can be drawn for a bank to be able to prepare for a crisis event:

- **Operational risk**
- Operational risk should be clearly defined and understood by all employees of the bank. Understanding operational risk will enable employees to identify specific risk factors that a crisis incident could expose the bank to, therefore allowing the bank to react appropriately by means of proactive control measures.

- **Risk management framework components**

A bank should develop and embed an operational risk management framework to serve as a platform for operational risk management. The identified components are as follows:

- **Risk management culture**

- A risk culture should ensure the embedding of norms, attitudes and behaviours of employees relating to risk controls.

- **Risk management structure**

- A governance structure should be embedded to confirm the roles and responsibilities of role-players in risk management.

- **Risk management strategy**

A risk management strategy should be aligned with the business strategy to ensure that the objectives are within the set parameters of the risk appetite.
 - **Risk management process**

A risk management process should be formalised and embedded in the organisation. The steps of a risk management process are as follows:

 - Risk identification should be a step of an operational risk management process to identify inherent risk exposures.
 - Risk evaluation should be a step of an operational risk management process to assess the identified risks in terms of likelihood and impact.
 - Risk control and mitigation should constitute a step of an operational risk management process to establish risk control measures for the identified risks.
 - Risk monitoring should constitute a step of an operational risk management process to ensure the continuous monitoring and reporting of risks and control measures.
- **Operational risk factors**
 - **People risk**
 - Organisations should appoint employees who are responsible for identified critical functions during a crisis event.
 - Employees should be trained to understand and perform their functions during a crisis event.
 - Organisations should ensure a healthy and safe environment for employees during times of crisis.
 - **Process risk**
 - Organisations should develop adequate policies and procedures to ensure the continued operation of business processes during times of crisis.
 - Policies and procedures should stipulate effective communication strategies between all stakeholders to ensure the flow of essential business information to ensure continued business operations.
 - A business continuity management policy should be approved and include a detailed business continuity planning process that addresses a crisis.

- **System risk**
 - A cybersecurity policy should include a process to ensure data and information security.
 - A continuous training communication process should be established to inform all stakeholders on cyber activities or threats.
 - A data backup facility should be established to protect an organisation from losing critical data due to a disruption caused by a crisis event.

- **External risk factors**
 - A BCM should be developed to ensure business continuity during a crisis.
 - The BCM should include all stakeholders responsible for business continuity during a disruption.
 - The BCM should include a process for dealing with a crisis that could disrupt the business or threaten the safety of employees.
 - A BCP should be defined to ensure that all stakeholders understand their roles and responsibilities during a crisis.
 - Training drills should be used to test the effectiveness of the BCP.
 - The BCM should identify critical functions of an organisation that should remain operational during a crisis.
 - A BCP should stipulate which functions can be performed remotely during a crisis event.

Defining and clearly understanding the operational risk of a bank and embedding a risk management framework could serve as a platform for effective risk management. The literature review revealed that it is important for banks to proactively prepare for crisis events. In this regard, BCM, cybersecurity and data protection are important tools for protecting banks against crisis events. The next chapter will provide a detailed overview of the research methodology used to achieve the secondary objective of an empirical analysis of the identified control measures for operational risk to protect banks against crisis events and to determine the current applicability of the identified controls. The findings of the empirical analysis will be used to confirm the conclusions and serve as a platform for recommendations to achieve the objectives of the study.

CHAPTER 4: RESEARCH DESIGN AND METHODOLOGY

4.1. Introduction

Chapter 2 provides an overview of operational risk, while Chapter 3 examines COVID-19 in terms of operational risk factors. The outcomes from the empirical analysis will be used to confirm the conclusions derived from the review of the literature and provide an opportunity for recommendations to answer the following research question: what appropriate operational risk control measures are available for the Lesotho banking industry to adopt in preparation for future crisis events? This chapter explains the research design for the study to establish an outline of how the study will be executed to achieve the objectives, which will provide a response to the research question.

4.2. Research Design

A research design is the broad strategy of how the study's research questions will be addressed, indicating the sources from which the data will be acquired, how the data will be gathered and evaluated, and principled issues and limitations (Sekaran & Bougie, 2013). Creswell (2014) defined research design as the plan, structure, strategy, and investigation conducted to address the research question and control variance. A research design, according to Creswell and Creswell (2023), is the design of conditions for data collection and analysis via an approach that seeks to combine relevance to the research purpose with economy and method. According to Bryman, Bell, Hirschsohn, Santos and Toit (2014), research design is a structure and framework for data collection and analysis. Creswell (2014) stated that it is critical for a researcher to select a suitable research design. Bryman et al. (2014) also stated that a research design is required to ensure that various research techniques are effective, which leads to professional research that generates the most information with the least amount of effort, time, and money. According to Saunders and Tossey (2013), understanding the context and aim of a research design is crucial for a researcher. A researcher may conduct descriptive, exploratory, or explanatory research. This review of the aforementioned research design serves as a guide for selecting a suitable design for this study.

4.2.1. Descriptive research

Descriptive research is used to identify and collect data on aspects of a certain subject, such as characterising social occurrences, social structures, and social circumstances (Bloomfield & Fisher, 2019). Kumar (2011) defined descriptive research as the systematic description of a situation, problem, phenomenon, or service. According to Bloomfield and Fisher (2019), descriptive research studies the current situation and is used to identify the characteristics of a particular issue. Descriptive research investigates the situation as it is; it can be used to determine variable features or the extent to which variables exist in a certain context or

circumstance (Salkind, 2019). Descriptive research, which can be quantitative, qualitative, or mixed methods in nature, is used to investigate the existing conditions (Kumar, 2011).

4.2.2. Exploratory research

Exploratory research is a primary stage of research that aims to achieve new insights into a phenomenon (Myers, Arnold, Robert & Lorch, 2010). An exploratory study is concerned with a topic for which no hypotheses have been developed. The researcher's role is to review the available material towards constructing a hypothesis from it. This concept may have been stated in prior research papers in some sections of the subject topic. Researchers must test these various hypotheses to assess their value for future research and determine whether they generate new ideas (Sekaran & Bougie, 2013). According to Sekaran and Bougie (2013), exploratory research is primarily determined by secondary research (such as a literature review) and qualitative data collection methods such as unconfirmed discussions or formal data collection methods such as case studies or interviews.

4.2.3. Explanatory design

Explanatory research is a study that aims to investigate a previously unknown cosmos (Kumar, 2011). According to Collis and Hussey (2014), explanatory research is a continuation of descriptive research in that it analyses and explains how or why the phenomenon exists rather than simply identifying the aspects of the problem. Myers et al. (2010) further indicated that explanatory research intends to understand why an incident occurs.

The aim of this study is to determine operational risk control measures to prepare and safeguard banks from potential operational risk exposures during crisis events based on the experiences of the COVID-19 pandemic. Therefore, a descriptive design will be used to investigate the effect that the COVID-19 pandemic has had on the operational risk faced by the banking industry to establish appropriate operational risk controls and mitigations that the Lesotho banking industry can adopt to prepare for future crisis events.

According to the preceding discussion, studies must have a plan developed for how the study will be carried out. This research conforms to the research onion recommended by Saunders, Lewis and Thornhill. (2012). According to Alturki (2021), a research onion is a framework for determining the right methodology. Figure 4.1 below shows the research onion by Saunders et al. (2012) that was adopted for this study.

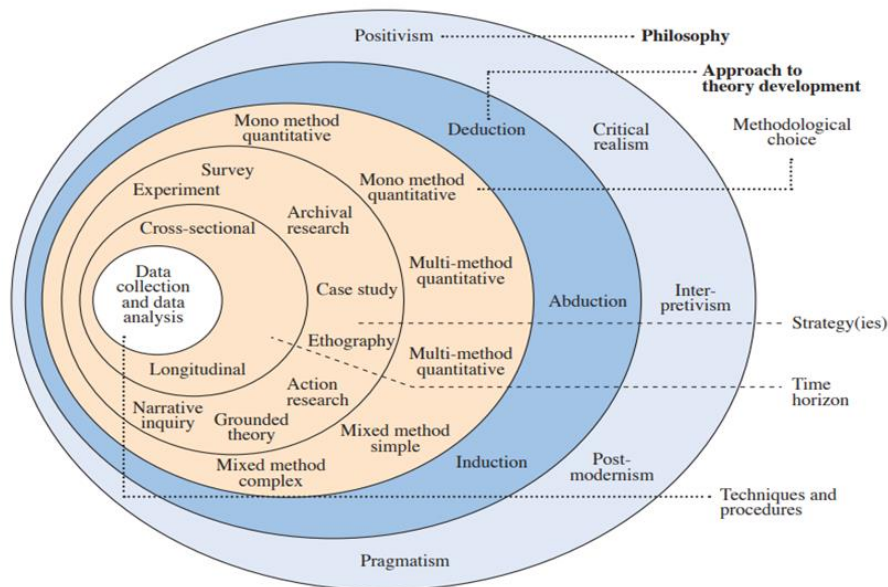


Figure 4.1: Research onion

Source: Saunders et al. (2012)

The layers of the framework in Figure 4.1 converge on a different view of the study, demonstrating the scope of the research philosophy and paradigms, research approach, methodology choice, research strategies, time horizon, population and sample size, data collection, and analysis techniques used in the study. These steps of the research design will be covered in the subsequent sections to determine an appropriate approach for this study.

Researchers must be able to comprehend and express concepts about the nature of reality, what can be learned about it, and how to obtain this information (Rehman & Alharthi, 2016). These are characteristics of research paradigms, which will be examined further below.

4.3. Research Philosophy/Paradigm

Rehman and Alharthi (2016) defined philosophy, which is also known as a paradigm, as a fundamental belief system and theoretical framework based on assumptions. Creswell (2014) defined research philosophy/paradigms as a fundamental set of assumptions that influence action. According to Saunders et al. (2012), philosophy is the advancement and development of understanding. The first layer of the research onion has been widely accepted in educational research. For example, Creswell (2014) noted that there are four research philosophies: post-positivism, constructivism/interpretivism, realism, and pragmatism. Bryman et al. (2014) examined three major viewpoints: positivist, interpretivism, and realism. Kivunja and Kuyini (2017) identified positivists, interpretivists, constructivists, transformative, and pragmatics as

significant research paradigms. As a result, positivism, post-positivism, interpretivism, realism, and pragmatics will be examined to guide the methodology approach adopted for this study.

4.3.1. Positivism

Saunders et al. (2012) defined positivism as a scientific technique of study. According to Sekaran and Bougie (2013), positivism is a scientific method that incorporates an experimentation method that is used to investigate observations and answer questions. Myers et al. (2010) noted that positivists believe that they can apply natural science methods to social science practices. Rehman and Alharthi (2016) concurred by stating that positivists attempt to comprehend the social world in the same way as they do the natural world. Bryman et al. (2014) defined positivists as those who design a rigorous process, collect quantitative data, and use descriptive and statistical approaches to test previous ideas. According to Myers et al. (2010), positivism research can be both quantitative and qualitative. However, owing to various criticisms levelled towards positivist research, Richard, Bond and Stokes-Zoota (2003) stated that while objective and scientific methods are suitable for researching natural objects, they are less effective when applied to social phenomena. Furthermore, Richard et al. (2003) argued that the intricacy of laws governing individuals, their unique characteristics and relationships, represents the order and regularity observed in nature. Therefore, post positivism emerged (Rehman & Alharthi, 2016). Post positivism will be discussed next.

4.3.2. Post positivism

Following various critiques of positivism, post positivism evolved. Creswell (2014) defined post positivism as a study that demonstrates the need to recognise and evaluate the sources that have an impact on outcomes. Post positivism is reductionist in the sense that it aims to break down ideas into smaller variables composed of theories and research problems (Creswell, 2014). Furthermore, as stated by Panwar, Ansari, and Shah (2017), post positivism focuses on exploring ideas within the framework of involving the majority's experiences and announcing that the results of what the majority says are acceptable. According to Henderson (2011), post-positivism emphasises meaning rather than explaining social concerns. These methods provide a practical approach to data collection by employing multiple methods. Creswell (2014), on the other hand, contended that post positivism's assumptions are more correct in quantitative research than in qualitative research. Post positivism, according to Manjikian (2013), enables researchers to be flexible about their perspective on a topic they find fascinating to study.

4.3.3. Interpretivism

Typically, interpretivism is qualitative. It aims to comprehend the subjective state of human experience and strives to become a part of the subject being researched, comprehending and interpreting what the subject contemplates (Creswell & Cresswell, 2023). Saunders et al. (2012) stated that when employing this approach, researchers are not excluded from the case

study under investigation; instead, they regard themselves as participants in the situation under investigation. Interpretivism, according to Bryman et al. (2014), focuses on conducting research among humans rather than among objects. Furthermore, they assume that any study approach in natural science must recognise the distinction between humans and objects.

4.3.4. Realism

A realism researcher, according to Saunders et al. (2012), interacts with the participants. According to Salkind (2019), realist researchers examine concerns about power, oppression, and trust among participants. Furthermore, depending on the topic, realism research can be quantitative or qualitative (Saunders et al. 2012). Realism researchers aim to discover the relationships among politics, morality, and ethics. Additionally, the researcher promotes human rights and social justice and cooperation through transformative research (Kivunja & Kuyini, 2017). According to realism research, experiences are sensations and representations of what one encounters in everyday situations, not what is real (Kivunja & Kuyini, 2017).

4.3.5. Pragmatism

According to Kivunja and Kuyini (2017), pragmatic research simplifies the reality that no single scientific method can provide access to real-world information. Saunders et al. (2012), on the contrary, contended that this does not indicate that pragmatists must always employ a mixed approach; rather, the method selected depends on the objective of the research. Therefore, pragmatism enables the researcher to address the questions under investigation without considering whether they are quantitative or qualitative. Furthermore, Saunders et al. (2012) indicated that pragmatists search for important points of connection within the research work to assist in understanding the context. Creswell and Cresswell (2023) also stated that pragmatism develops from actions, situations, and consequences.

The positivist paradigm is the subject of this study because the proposed theories stated in this paradigm are for quantitative research. Positivists advocate the use of descriptive and statistical methods to test previous hypotheses. Positivism simplifies a greater circle of concepts into smaller, distinct variables such as hypotheses and research questions (Cresswell, 2014). This study raises the question of “what operational risk control measures are most appropriate for safeguarding banks from operational risks during a crisis event?” It aims to compare the confirmed operational risk control measures with the current applicability of those controls within the bank, which fits a description of positivism research; therefore, positivism seems appropriate for this study. The following section discusses the research approach.

4.4. Research Approach

The research approach is the next layer of the research onion and is utilised to establish whether the study argument progresses from unspecific to specific. According to Saunders et

al. (2012), the scope to which a study is distinct about the theory at the start of the investigation raises a crucial question regarding the study's rationale. A researcher can use one of the following three types of reasoning: deductive, inductive, or abductive.

4.4.1. Deductive approach

Deductive reasoning represents the common concepts regarding the type of relationship that exists between research and theory. It is an approach appropriate for testing/verifying an existing theory about the relationships between variables (Bryman & Bell, 2011). According to Sekaran and Bougie (2013), deductive reasoning starts with the broad and progresses to the specific. It begins with the identification of a wide range of problem areas, followed by the definition of the problem statement, hypothesising, identification methods, data collection, and data and results analysis. According to Saunders et al. (2012), deductive reasoning involves developing a hypothesis and subsequently designing a research strategy to test or confirm the hypothesis. In deductive reasoning, a theoretical structure is created and examined by experimental examination (Bryman & Bell, 2011). Deductive reasoning effectively expresses arguments based on laws, rules, or other widely accepted principles. As stated by Bryman and Bell (2011), a deductive approach is often used to conduct quantitative research.

4.4.2. Inductive approaches

Inductive reasoning is defined as moving from the specific to the general. A specific phenomenon is identified in inductive research to obtain a general conclusion or develop a framework (Sekaran & Bougie, 2013). According to Saunders et al. (2012), inductive researchers work from the bottom up, embracing participant perspectives to construct broader areas and generate a theory. These inductive approaches start with the research questions, aims and objectives that need to be addressed during the research process, beginning with the data collection. Sekaran and Bougie (2013) further indicated that arguments based on experience or observation are successfully expressed using inductive methodologies. Unlike the deductive approach, the inductive approach is commonly used for qualitative research (Sekaran & Bougie, 2013).

4.4.3. Abductive approach

When developing a new rationalised theory or deconstructing, modifying, or rationalising an existing theory concerning the relationship between dependent and independent variables in a research problem, an abductive approach is applicable (Bryman & Bell, 2011). Saunders et al. (2012) agreed and discussed how an abductive approach is applied to investigate a phenomenon, discover themes, and clarify models to develop an additional or transform existing theory that is then assessed through additional data collection. According to Bryman and Bell (2011), abductive reasoning aims to explain incomplete observations, unexpected facts, or riddles that were presented at the beginning of the study but are not addressed by

the current hypothesis. An abductive approach is utilised in both quantitative and qualitative research.

This study's primary objective is to identify the effect of the COVID-19 pandemic on the operational risk faced by the Lesotho banking industry to determine preventative control measures. To achieve this objective, this study conducted a literature review on operational risk to identify possible control measures. Furthermore, the COVID-19 pandemic was analysed in terms of confirmed operational risk factors linked with the identified control measures. The data will be collected from the three banks in Lesotho and analysed to determine the findings, which will serve as a basis for recommendations. Therefore, a deductive approach was used for the purposes of this study.

4.5. Methodological Choice

The third layer of the research onion refers to a methodological choice, which involves deciding among various study research approaches. Creswell and Creswell, J.D. (2023) defined the research method as the procedure adopted by the researcher to collect, evaluate, and interpret the data for the study. According to Saunders et al. (2012), methodological approaches can be quantitative, qualitative, or hybrid (mixed method). The abovementioned approaches will be briefly discussed with the intent of determining the most appropriate approach for this study.

4.5.1. Quantitative research

According to Saunders et al. (2012), quantitative research is an analysis method or collection approach that creates or practices numerical data for examination in a research study. The method of performing quantitative research commences with the researcher choosing a topic (Saunders et al., 2012). Quantitative researchers usually begin with a broad topic of study or an issue of professional or personal interest. Researchers then narrow it down or focus on a specific research question that the study can address. A thorough analysis of the literature and the creation of hypotheses from social theory are often employed to achieve the latter. According to Creswell (2014), quantitative studies employ theory deductively and place the literature review at the beginning of the research with the aim of testing or proving a theory rather than constructing it. The theory will then serve as the study's framework, the research questions and the data collection procedure. For quantitative research, data collection methods such as questionnaires could be used. Quantitative researchers use close-ended questions. Although a quantitative approach may still be used within pragmatics and transformists, it is mostly associated with a positivism paradigm (Saunders et al. 2012).

4.5.2. Qualitative research

Qualitative research is a social or behavioural science study that employs exploratory approaches such as interviews and surveys to explore the processes that govern human

behaviour (Creswell & Creswell, 2023). Qualitative researchers begin with self-evaluations and reflections on their own position in a social-historical setting (Kumar, 2011). Like a quantitative researcher, a qualitative researcher designs a study, collects, analyses, and interprets data (Kumar, 2011). However, qualitative researchers commonly use interviews as data collection tools, and the data analysis procedure is nonnumerical (Apuke, 2017). In addition, qualitative research is context-dependent and often associated with interpretivism. A qualitative method can be employed for transformational and pragmatic research designs (Saunders et al., 2012). Unlike quantitative researchers, who examine hypotheses, qualitative researchers construct their own hypotheses (Salkind, 2019). The aim of qualitative research is to study, comprehend and recognise participants' values, circumstances, emotional states, incidents and ideas (Kumar, 2011). Qualitative research is not a substitute for quantitative research; rather, it is a different approach that allows researchers to ask and answer different kinds of questions. Qualitative researchers use open-ended questions (Creswell, 2014).

4.5.3. Mixed methods

The mixed method is an extension rather than a replacement for quantitative and qualitative methods. It combines the collection and analysis of data methodologies from quantitative and qualitative research approaches in a single study (Salkind, 2019). A mixed-methods approach, according to Creswell and Creswell (2023), employs quantitative data to collect statistical and qualitative data to collect words without allocating each method to a specific research paradigm. For example, for the same study, a researcher may distribute a survey with closed-ended questions to collect numeric or quantitative data and conduct an interview with open-ended questions to collect narrative or qualitative data. Researchers who use a mixed methods approach aim to take advantage of the capabilities of both quantitative and qualitative research approaches (Creswell & Creswell, 2023). Apuke (2017) associated mixed method research with transformative research, which prioritises quantitative data analysis over qualitative research methodologies aimed at examining perceptions. Mixed methods research is further beneficial to pragmatism, which values both quantitative and qualitative research depending on the nature of the study (Salkind, 2019).

For this study, a quantitative approach will be used because the study will collect data using closed-ended questions to assess the importance of the identified operational risk controls to compare with the current applicability of such controls by banks in Lesotho.

4.6. Research Strategy

The research strategy is the fourth layer of the research onion. According to Saunders et al. (2012), a research strategy is a plan that a researcher will follow to answer a research question and achieve the study's objectives. A research strategy assists in the research design and execution and monitoring of the study (Saunders et al., 2012). There are various methods

available for conducting quantitative, qualitative, or mixed research. Creswell (2014) suggested that the techniques employed to collect quantitative data include experiments and surveys, which will be used next to identify the best tools for this study.

4.6.1. Experiments

According to Taheri, Porter, Valantasis-Kanellos and König (2015), experiments have a wide range of applications in social research. They are regarded as dependable and efficient in terms of data collection and theory verification (Taheri et al., 2015). Taheri et al. (2015) stated that the experimental data collection method is used to determine whether a change in an independent variable induced by data manipulation affects the dependent variable. In contrast, Sekaran and Bougie (2013) asserted that experiments generally identify casual connections between variables. According to Sekaran and Bougie (2013), the essence of an experiment is that the study scenario is one that the researcher creates. As a result, it allows for great control over the design and technique, allowing for broad interpretation. According to Bryman et al. (2014), experiments are usually carried out in laboratories or in real-world settings. According to Taheri et al. (2015), laboratory studies are partially artificial. Experimenters variables that are easily managed over variables that reflect the daily routines of people confronted with contemporary issues. There are three experimental research designs:

4.6.2. Pre-experimental designs

Pre-experimental designs are not distinguished by random selection and they do not have a control group. As a result, the potential of such designs to reveal the random nature of the relationship between variables is reduced if not eliminated. Pre-experimental design provides little or no control over independent variables that could be responsible for findings that differ from those planned by the researcher (Salkind, 2019).

4.6.3. True experimental designs

True experimental designs comprise methods for randomly selecting and assigning individuals, including a control group, which strengthens the argument in support of a relationship between cause and effect. True experimental designs are considered strong because they involve random participant selection, random treatment assignment, and random group assignment (Salkind, 2019).

4.6.4. Quasiexperimental designs

In a quasiexperimental design, the hypothesised logic of differences between groups observed by a researcher has already occurred. Therefore, group assignment has already taken place (Salkind, 2019).

4.6.5. Survey

Survey research involves collecting information from a sample of people based on their responses to questions (Ponto, 2015). According to Ponto (2015), survey research can employ

quantitative methods such as questionnaires, qualitative methods such as open-ended questions, or both in a mixed-methods study. According to Salkind (2019), survey research is intended to gather both primary and secondary data from a sample with the aim of statistically assessing the data and generalising the conclusions to the population. According to Singleton and Straits (2009), surveys are often employed in social and psychological research because of their efficiency in prompting human behaviour. This finding is consistent with Sekaran and Bougie's (2013) view, who stated that survey research looks at the frequency of correlations between psychological and sociological variables, as well as constructs including attitudes, beliefs, prejudices, preferences, and views. The survey research plan, according to Ponto (2015), begins with the study purpose, proceeds to various methods that may be employed to collect data, and concludes with a final report and summary of findings. Ponto (2015) mentioned that a questionnaire is an appropriate data collection tool that can be employed in survey research. The questionnaire will be explained further in the following sections.

As stated in Chapter 1, this descriptive study will use a quantitative method and focus on the positivism paradigm. Based on the discussion of quantitative data collection approaches, primary data in the form of a questionnaire will be employed to determine the effect of the COVID-19 pandemic on the operational risk faced by the banking industry to identify and confirm the operational risk control measures for the Lesotho banking industry to be prepared for crisis events. The survey approach seems adequate for this study because a representative population sample will be employed to collect primary data for empirical analysis from self-administered questions. The questionnaire was designed based on conclusions drawn from the literature review and from the COVID-19 pandemic using close-ended questions.

4.7. Time Horizon

The time horizon is the fifth layer of the research onion. According to Saunders et al. (2012), the time horizon refers to the duration of the research. The period during which research was conducted might be either cross-sectional or longitudinal (Salkind, 2019). According to Salkind (2019), the cross-sectional method investigates various groups of people at the same time. Furthermore, because the testing duration is brief, cross-sectional methods are cost effective, and dropout is limited (Saunders et al., 2019). Nonetheless, Saunders et al. (2019) state that it takes a considerable amount of time to complete this type of project because people tend to be positioned in the same location. Cross-sectional designs involve surveys that collect data through questionnaires or structured interviews. The longitudinal method, on the other hand, evaluates the behaviour of a single group of participants over time (Salkind, 2019). According to Saunders et al. (2012), longitudinal studies are being conducted to investigate age changes over time. As a result, longitudinal research allows for the study of development over time

(Salkind, 2019). A longitudinal design enables a researcher to assess the trend of change and obtain data, necessitating regular collection and therefore ensuring its accuracy (Kumar, 2011). This study adopts a cross-sectional method because of time constraints and because it is cost effective. The following section discusses the techniques and procedures of the study.

4. 8. Techniques and Procedures

The final layer of the research onion denotes the techniques and procedures to be adopted to collect and analyse data, which Saunders et al. (2012) regarded as the core of the research onion. This section focuses on the population of the study, sampling technique, data collection and data analysis that will be used in this study.

4.8.1. Study population

According to Sekaran and Bougie (2013), the population is a group of potential participants to whom the researcher wants to generalise the results of the study. As indicated in Chapter 1, the population consisted of the four banks in Lesotho: Standard Lesotho Bank, First National Bank, Nedbank and Lesotho Post Bank. The four banks are regulated by the Central Bank of Lesotho under the Financial Institutions Act, 2012 and other related laws. However, the Central Bank of Lesotho also provides banking services for the government. The following section justifies the sample technique that was employed in this study.

4.8.2. Sampling technique

A sample is a smaller group selected from the population to participate in the study due to constraints such as time and money (Sekaran and Bougie, 2013). According to Salkind (2019), samples should be selected from the population in such a way that the researcher reduces the probability that the sample represents the population as much as possible. The intention is to have the sample representative of the population so that, when the research is completed, the sample-based results can be generalised to the population. The quantitative data collection strategy used in this study involved selecting the sample size based on the factors considered and the available resources. According to Kumar (2011), various sampling techniques are available for quantitative research. Therefore, the next section discusses available sampling techniques to determine the most appropriate sampling technique for this study.

4.8.2.1. Probability sampling strategy

Probability sampling strategies are the most commonly employed because participant selection is determined by chance. That is, participants' selection is determined by non-systematic and random rules, where the possibility of the sample representing the population is strengthened. Several authors have identified simple random, systematic, stratified, and cluster sampling as primary techniques for selecting probability sampling (Salkind, 2019; Ajayi,

2017; Kumar, 2011; Sekaran & Bougie, 2013). Saunders et al. (2012) stated that the most common type of probability sampling procedure is simple random sampling.

4.8.2.2. Simple random sampling

Each member of the population has an equal and independent probability of being selected to be a part of the sample via simple random sampling (Saunders et al. 2012). According to Saunders et al. (2012), simple random sampling does not require preconception because one individual may be chosen over another, and the choice of one person does not bias the researcher in favour of or against the choice of another. Simple random sampling is associated with survey research methodologies in which a researcher must conclude inferences about a population from the sample to accomplish the research's aim and answer a research question (Kumar, 2011). According to Salkind (2019), the researcher who employs a simple random sample first chooses the population from which the sample will be selected, lists all members of the population and assigns numbers to each member. The researcher will then apply the criteria to choose the sample.

4.8.2.3. Nonprobability sampling strategies

According to Sekaran and Bougie (2013), the probability of selecting a single individual is uncertain in nonprobability sampling. A researcher must assume that possible members of the sample do not have an equal and independent chance of being selected when using nonprobability sampling (Sekaran & Bougie, 2013). Nonprobability sampling, according to Kumar (2011), may be employed in both quantitative and qualitative research. In quantitative research, the researcher chooses a predetermined sample size, while in qualitative research, the researcher does not determine the number of people who will respond in advance but instead continues to choose additional cases until the researcher reaches the data saturation point (Kumar, 2011). When undertaking nonprobability sample research, certain methods include quota, convenience, accidental, purposive, and volunteer sampling (Sekaran & Bougie, 2013; Saunders et al., 2012).

Based on the review of the sampling strategies above, a nonprobability sampling method was applied for this study. As indicated by Kumar (2011), nonprobability sampling allows the researcher to make his or her own judgement as to who will provide sufficient information that will assist in achieving the objective of the study. Nonrandom sampling will allow the researcher to focus on specific participants who will be able to provide information that the researcher seeks (Sekaran and Bougie, 2013). This study investigates the effect of the COVID-19 pandemic on the operational risks faced by the banking industry to identify operational risk control measures for the Lesotho banking industry to adopt to prepare for future pandemics. Therefore, three banks (the Nedbank, Post Bank and Central Bank of

Lesotho Banking Operations) participated in this study. The sample will be drawn from the participants across a variety of appropriate roles within the banks, for example, business officers and managers in risk management, compliance and other officers and managers who work directly with operational risk management in the banks.

4.8.3. Data collection

The data are a set of values for qualitative and quantitative characteristics that can be used to draw conclusions. A researcher must collect and sort data to present and evaluate it (Ajayi, 2017). Ajayi (2017) recognises two ways in which data can be collected: primary data collection and secondary data collection. The following are definitions of the data collection methods used by Sekaran and Bougie (2013):

- Primary data are first-hand information gathered by the researcher using tools such as surveys, questionnaires, focus groups, interviews, observations, and case studies.
- The secondary data were previously acquired by another party who was not related to the current investigation. Case study records, online data, materials, published or unpublished data, government sources, library reports, company websites, and previous research are examples of secondary data sources (Sekaran & Bougie, 2013). Secondary data sources, according to Saunders et al. (2012), are not the original reporting.

This study collected primary data in the form of a survey. According to Ponto (2015), the most generally used instrument for survey studies is a questionnaire. Therefore, the next section addresses a questionnaire as a data collection instrument.

4.8.3.1. Questionnaire

A questionnaire is a tool used by researchers to collect information from respondents (Saunders et al. 2012). According to Ponto (2015), questionnaires can be used for performing quantitative research. The questions on the questionnaire, according to Sekaran and Bougie (2013), are organised in such a way that participants can complete them on their own. A questionnaire allows for standardised data collection from a large population, and it is cost effective (Saunders et al., 2012). However, Kumar (2011) argued that a questionnaire method could be limited by, among other factors, a lack of opportunity for clarity, not providing unstructured responses, or not allowing participants to support their responses. A questionnaire is an efficient way of collecting responses from a large sample because each participant is asked to respond to the same question (Kumar, 2011). Kumar (2011) highlighted several important points that researchers must consider when developing a questionnaire:

- A questionnaire must be designed in such a way that its demand for time, expense, and effort is reasonable. Personal questions must be avoided.

- A questionnaire must be designed to accomplish the researcher's goal not to collect information on a related but implicit topic.
- A questionnaire must contain interesting questions that encourage respondents to participate.

This study collected primary data utilising a questionnaire. The questionnaire allows respondents to answer questions at their own free time, relieving both the researcher and the respondent of stress. A questionnaire ensures that the collected data are consistent because each respondent is asked the same questions (Kumar, 2011). The questionnaire used for this study (Annexure A) has the following structure:

- **Cover letter**

A cover letter was included with the questionnaire, which was used to introduce the study, state the title and purpose of the study and explain the details of the questionnaire. It includes time estimations so that the participant can know when to return it. Additionally, the cover letter indicates that participation is voluntary, that confidentiality and anonymity are guaranteed and that there will be no monetary compensation for participation. The study also received written approval from the UNISA Research Ethical Review Committee. The cover letter is included as Annexure B in this study.

- **Consent to participate in the survey**

The consent form included in this study, Annexure C, will be shared with the participants. By completing and signing the form, the participants provided consent to participate in the survey.

- **Instructions**

The questionnaire will provide clear instructions on how the participant should complete it.

- **The main body**

The main body consists of actual questions. The survey consists of questions based on conclusions about operational risk controls during a crisis and was derived from the analysis of the COVID-19 pandemic in relation to operational risk factors in Chapter 3. Questions 1 to 4 relate to biographical information to determine the respondents' focus areas and years of experience, determining whether they fall within the relevant requirements for this research, as indicated in Section 4.8.2.3.

According to Ajayi (2017), using a five-point Likert scale generates reliable quantitative data that can be easily examined, provides a lower margin of error, and gives respondents a choice without overwhelming them. Therefore, the questionnaire contains close-ended questions answered on a five-point Likert scale: 1= to no degree, 2= to a lesser degree, 3= to moderate degree, 4= to a degree and 5= to a full degree. The questions of the questionnaire were divided into two sections. Section A requires respondents' views on the significance of operational risk controls that were identified during a literature review and analysis of the COVID-19 pandemic.

Section B seeks respondents' views on the current applicability of identified control measures. The questionnaire was attached as an annexure and emailed to prospective participants with a cover letter. The section that follows describes the questionnaire's pilot-test.

4.8.3.2. Pilot-testing

Pilot-testing is a stage in the development of a questionnaire that determines the potential effectiveness of the questionnaire (Bryman & Bell, 2011). The questionnaire was pilot-tested to ensure that it met the objectives of the study (Bryman & Bell, 2011). The questionnaire was distributed to consult professionals in operational risk management within financial institutions other than banks. The feedback received addressed the representational accuracy, design, and content and appropriateness of the questions. The relevant comments and suggestions from the experts were incorporated into the final questionnaire (refer to Annexure D) before it was distributed to the sample population for the actual survey.

4.9. Data Analysis

After the data were collected via a questionnaire survey, they were analysed and interpreted (Creswell, 2014). According to Creswell (2014), the data analysis method is determined by the research approach. Since this study adopts a quantitative approach, descriptive and inferential statistics are appropriate. Descriptive analysis indicates components of the distribution of scores obtained to provide an appropriate initial illustration of what the data look like (Myers et al., 2010). After the results were explained, inferential statistics were used to compare groups A and B and to substantiate the relevant conclusions. (Myers et al., 2010). According to Salkind (2019), statistics provide a method of describing collected quantitative data that readers comprehend, thus allowing the research outcome to be used for evidence-based practice and therefore narrowing the theory. Salkind (2019) highlights that the type of data collected, as well as its analysis or representation, must be appropriate so that the research question may be answered meaningfully, and that knowledge can be retrieved from the collected data.

For this study, the data collected from the sample were statistically analysed with Microsoft Office Excel 2016 to calculate averages, percentages, and standard deviations. Each question has two answers. Therefore, the results obtained from Section A of the questionnaire, which confirms operational risk controls for banks during a crisis, will be compared with the results from Section B, which indicates the current applicability of those controls, to identify a research gap. The researcher will then base the findings and recommendations on the research gap obtained from the comparison of the two sections.

4.9.1. Data measurement

As stated in Chapter 1, Section 1.6.5, reliability and validity are significant indicators of a measuring instrument's quality (Cooper & Schindler, 2008). Kumar (2011) indicated that it is critical to determine the validity and quality of the tools employed in a survey to answer a research question.

4.9.1.1. Validity

According to Saunders et al. (2012), validity is the extent to which an instrument measures what it is supposed to measure. According to Creswell (2014), validity is an instrument's ability to measure the significance of imperial thoughts and determine the degree to which the significance can be regarded as true. According to Taherdoost (2016), validity demonstrates how effectively the data collected cover the actual areas of inquiry. Kumar (2011) classifies validity into three types: face and content validity, criterion validity, and construct validity.

4.9.1.2. Face and content validity

The degree to which a measure appears to be related to an assigned construct is referred to as face and content validity (Kumar, 2011). Face and content validity pertain to how well the items developed to operationalise the construct provide a sufficient and representative sample of all the items that could measure the construct of interest (Taherdoost, 2016). According to Taherdoost (2016), face and content validity mainly depend on the judgement of experts in the field to assess the alignment between the questions asked and the objective of the research.

4.9.1.3. Criterion validity

Criterion validity is concerned with how well a test estimates current performance (concurrent validity) or predicts future performance (predictive validity) (Salkind, 2019). According to Taherdoost (2016), a test has criterion validity if it predicts performance or behaviour in another scenario (past, present, or future). Criterion validity demonstrates how well the new measure correlates with other measures of the same contrast (Kumar, 2011).

4.9.1.4. Construct validity

Construct validity is defined as the degree to which test findings are related to an underlying set of related variables (Saunders et al., 2012). Construct validity is characterised as the accumulation of evidence from multiple investigations conducted with a specific measuring instrument (Creswell, 2014). According to Taherdoost (2016), construct validity relates to how well the researcher translates or adapts a construct's concept, idea, or behaviour into a working and operational reality or execution.

For this study, the validity of the content was considered through face and validity content validity tests. The questionnaire included questions based on the literature. After assessing the actual questionnaire, professionals in operational risk management will be required to

complete the analytic questionnaire to assess the questionnaire's content and validity. The test will ensure that the questions and the study's objectives are in alignment. The results of the questionnaire pretest are presented in Annexure D.

4.9.1.5. Reliability

Creswell (2014) defined reliability as the extent to which a method's replication would yield similar results at different times. De Villis (2011) defined reliability as the extent to which a measurement of an occurrence produces steady and consistent results. Reliability testing is important since it pertains to the consistency of a measuring instrument's parts (De Villis, 2011). According to Kumar (2011), while reliability is important in research, it is insufficient unless it is supplemented with validity. That is, a test must be both credible and accurate to be considered reliable. Creswell (2014) set out four reliability techniques for testing the reliability of research findings:

- **Test-retest reliability**

Test-retest reliability is defined by Saunders et al. (2012) as a measure of how stable a test is over time. According to De Villis (2011), test-retest reliability is used to assess the consistency of measurements administered at different times to the same group or using the same criteria. The answer is dependent on how the researcher aspires to use the test results and the objective of the study (De Villis, 2011).

- **Parallel-form reliability**

In parallel, various versions of the same test were administered to the same group of participants. The results from the two tests are subsequently compared. The tests are said to be equivalent if the correlation between them is statistically significant, which means that the link is due to something shared by the two forms rather than a chance occurrence (Saunders et al. 2012).

- **Inter-rater reliability**

Interrater reliability is a measure of consistency between raters rather than between periods or tests (Saunders et al. 2012). According to Kumar (2011), interrater reliability confirms the equivalence of ratings acquired with an instrument when it is employed by various observers. To determine whether the raters agreed with one another, they rated their behaviour and calculated the percentage of agreement (Salkind, 2019). Interrater dependability necessitates separate ratings of the same event by multiple raters (Saunders et al., 2012).

- **Internal consistency reliability**

The internal consistency reliability estimates the equivalence of sets of test items (Saunders et al. 2012). Internal consistency, according to Creswell (2014), assesses

how unified items are in a test or assessment. The coefficient of internal consistency estimates dependability by assuming that items measuring the same construct are correlated (Salkind, 2019). Cronbach's alpha coefficient is the tool most often used for internal consistency (Salkind (2019)). Cronbach's alpha is determined by the average intercorrelations of the items as well as the number of items in the scale (Bonnet & Wright, 2015). It describes the accuracy of a sum of measurements, where the measurements reflect rates, events, alternate forms, or a questionnaire (Bonnet & Wright, 2015).

For this research, the internal consistency reliability test using Cronbach's alpha was employed because the data were collected by means of a questionnaire. The questionnaire consisted of closed-ended questions based on a five-point Likert scale. The scale items will consist of 1= to no degree, 2= to a lesser degree, 3= to moderate degree, 4= to a degree and 5= to a full degree. The Cronbach's alpha for the participants' questionnaires was 0.943. This indicates that there is perfect internal consistency on the item in the scale; hence, further analysis can be conducted. The results of the reliability test, calculated using the Cronbach's alpha coefficient, are provided in Annexure E.

4.9.2. Results of the validity tests

Introduction

The aim was to pretest the research questionnaire for this study for validity of the face and content methods, based on the literature review on validity and according to the conclusions in Chapter 4 Section 4.9.1.1. The questionnaire was subjected to a pilot by means of a group of experts in risk management. The experts were requested to evaluate the research questionnaire and complete the diagnostic questionnaire to ensure content and face validity. Table 4.1 shows the feedback from the pretesting of the questionnaire.

Table 4.1: Pilot questionnaire results

1. 1. The survey's purpose is distinct.								
Option	Strongly disagree	Disagree	Neutral	Strongly agree	Agree	Median	Average	Mode
	0%	0%	0%	50%	50%	4.5	4.5	4
2. 2. The questions are relevant to the study's purpose.								
Option	Strongly disagree	Disagree	Neutral	Strongly agree	Agree	Median	Average	Mode
	0%	0%	0%	50%	50%	4.5	4.5	4
3. The survey is inclusive in terms of operational risk controls for banks during a crisis event								
Options	Strongly disagree	Disagree	Neutral	Strongly agree	Agree	Median	Average	Mode
				25%	75%	4	4.25	4
4. The guidelines to complete the survey are distinct								
Options	Strongly disagree	Disagree	Neutral	Strongly agree	Agree	Median	Average	Mode
	0%	0%	0%	50%	50%	4.5	4.5	4
5. The questionnaire is constructed logically.								
Options	Strongly disagree	Disagree	Neutral	Strongly agree	Agree	Median	Average	Mode
	0	0	25%	50%	25%	4.5	4.25	5
6. The assertions are easy to understand.								
Options	Strongly Disagree	Disagree	Neutral	Strongly agree	Agree	Median	Average	Mode
	0	0	0	50%	50%	4.5	4.5	4
7. The survey's magnitude is adequate.								

Options	Strongly Disagree	Disagree	Neutral	Strongly agree	Agree	Median	Average	Mode
				50%	50%	4.5	4.5	4
8. Section A of the survey rates the importance of operational risk control measures that a bank should embed to effectively manage potential risks caused by a crisis event								
Options	Strongly disagree	Disagree	Neutral	Strongly agree	Agree	Median	Average	Mode
	0%	0%	0%	50%	50%	4.5	4.5	4
9. Section B determines the current applicability of the confirmed operational risk control measures in an organisation								
Options	Strongly disagree	disagree	Neutral	Strongly agree	Agree	Median	Average	Mode
	0%	0%	0%	25%	75%	4	4.25	4
10. Do you have any questions you'd want to include in the survey?								
Options					Response			
Yes					0%			
No					100%			
11. Indicate the time taken to complete the survey								
Option	0-5 min	6-10 min	7-15 min	16-20 min	21-25 min			
0%	25%	25%	50%	0%	0%			
12. Additional comments: No additional questions were added however, grammatical errors that were identified were corrected.								

Source: Author's own analysis

The table above shows the following:

- The aim of the survey is clear, where 50% of the respondents strongly agreed and 50% agreed, with a median score of 4.5, an average of 4.5 and a mode score of 4.
- The questions are aligned with the objective of the study, with a median score of 4.5, an average of 4.5 and a mode of 4, where 50% of the respondents strongly agree and 50% agree.
- The survey is extensive in terms of operational risk controls for banks during a crisis event, with a median score of 4, an average of 4.25 and 4 as the mode, where 25% of the respondents strongly agreed and 75% agreed.

- Fifty percent of the respondents strongly agreed, and 50% agreed that the guidelines for completing the survey were clear, with a median score of 4.5, an average of 4.5 and a mode of 4.5.
- The questionnaire was structured logically, with a median of 4.5, an average of 4.25 and a mode of 4, where 25% of the respondents were neutral, 50% strongly agreed and 25% agreed.
- The statements are simple to comprehend, with a median of 4.5, an average of 4.5 and a mode of 4, where 50% of the respondents strongly agree and 50% agree.
- The survey's magnitude is adequate, with a median of 4.5, an average of 4.5 and a mode of 4, where 50% of the respondents strongly agree and 50% agree.
- Fifty percent of respondents strongly agree, and 50% agree that Section A of the survey rates the significance of operational risk control measures that a bank ought to embed to effectively manage potential risks caused by a crisis event, with a median of 4.5, an average of 4.5 and a mode of 4.
- Twenty-five percent of the respondents strongly agreed, and 75% agreed that Section B determined the current applicability of the confirmed operational risk control measures in an organisation, with a median of 4, an average of 4.25 and a mode of 4.
- Fifty percent of the respondents strongly agreed, and 50% agreed that the survey was extensive regarding operational risk control measures for the bank during a crisis event, with a median score of 4.5, an average of 4.5 and a mode of 4.
- The time taken by participants to complete the questionnaire was approximately 5 to 15 minutes.
- All participants did not have additional questions.
- Some structural and editorial changes were recommended.

The recommendations were incorporated into the questionnaire; however, the feedback indicated that the questionnaire was valid for the study.

The next section addresses the ethical considerations of this study.

4.9.3. Ethical considerations

As discussed in Chapter 1, it is critical for researchers to treat human participants in the study with dignity, regardless of the research or outcome. Respect for a person in research, according to Ketefian (2015), assumes that human beings are independent; therefore, they must be respected. In compliance with the University of South Africa's (UNISA) ethical policy, the researcher will apply for ethical clearance from finance, risk management and banking departments before proceeding with the data collection and will attach ethical approval as Annexure F. General issues that a researcher must consider when conducting research are

highlighted in Chapter 1 as protection from harm, privacy, coercion, informed concern, confidentiality, and debriefing.

4.9.3.1. Protection from harm

Protection from harm entails ensuring that participants are protected from harm and discomfort. If there is a possibility that any harm occurs, the researcher must ensure that the participant is informed in advance (Saunders et al., 2012).

4.9.3.2. Informed consent

Informed consent was obtained by the researcher, who ensured that the participants voluntarily participated in the study without any pressure (Kumar, 2011). It is critical that the researcher explain to the participant the purpose of the study, what information is aimed for, and what the potential outcomes of the research are (Saunders et al., 2012). Before completing the questionnaire, participants will be required to read a consent form. The objective of the consent form is to guarantee participants' voluntary participation and confidentiality.

4.9.3.3. Deception

Deception is defined as the act of deceiving participants or denying information to create or conceal variables (Kumar, 2011). Such behaviours will be avoided in this study. To obtain accurate results or to protect personal data, researchers will avoid deceiving participants. The researcher will ensure that the individual's voluntary participation is not based on misinformation.

4.9.3.4. Privacy, confidentiality, and anonymity

Saunders et al. (2012) stated that confidentiality is essential in research. In other words, the researcher does not provide any information about one person to another. Participants' identities were not linked to the questionnaire to preserve anonymity (Saunders et al. 2012). Participation in this study will be fully anonymous; participants will not be required to reveal their identities, and the responses to the questionnaire will be password protected to prevent unauthorised access to the data. As a declaration, all individuals who have access to the data will sign a confidentiality form.

4.9.3.5. Coercion and incentives

The respondents were not manipulated to engage in the study (Salkind, 2019). The researcher did not provide any incentives for participating in the study.

4.9.3.6. Permission

A gatekeeper's letter was obtained from each bank (attached as Annexure G), which authorises the research to involve the Nedbank, Post Bank and Central Bank of Lesotho (banking operations) and their employees to participate in the survey. Two banks, the Standard Bank and First National Bank, declined to participate in the study, indicating that

they were unable to share the information required from the questionnaire in line with the banks' internal governing policies, such as information risk policies and the acceptable use of information assets.

4.10 Conclusion

This chapter examined the theory motivating the study's research strategy and methods. Figure 4.2 below depicts the customised research onion for this study, derived from the above discussions.

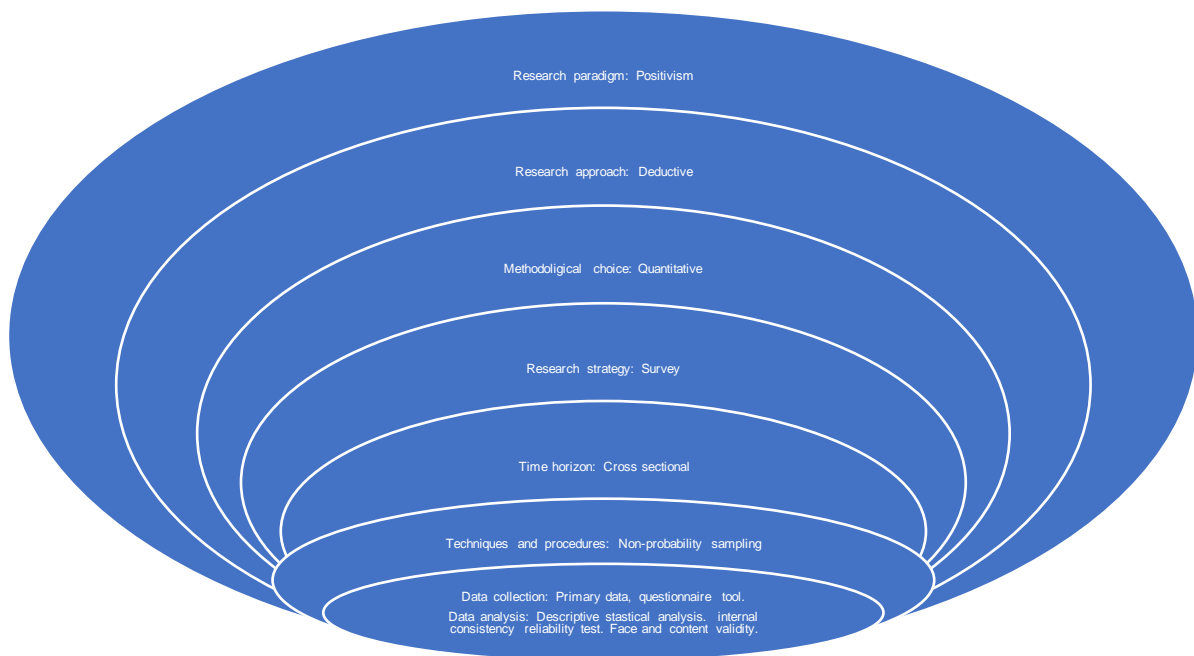


Figure 4.2: Adapted research onion

Source: (Author's own presentation of a research onion customised for this study and adapted from Saunders et al. (2012).)

The research design, approach, and strategic concepts were explained to determine the appropriate design, approach and strategy for this study. The objective of this study is to identify the effect of the COVID-19 pandemic on the operational risk faced by the Lesotho banking industry to determine preventative control measures. To achieve this objective, a quantitative research methodology was pursued. A questionnaire-based research strategy was chosen for this study. The questionnaire consisted of close-ended questions, and its validity and reliability were tested using face and content validity and internal consistency reliability tests. The targeted respondents are officers and managers of the bank who work directly with the operational risk of the banks: the Nedbank, the Lesotho Postbank and the Central Bank of Lesotho (banking operations). This study follows a descriptive research design because it aims to identify the effect of the COVID-19 pandemic on the operational risks faced

by the banking industry to determine preventative control measures, which fits the description of the descriptive research design that can be used to investigate existing conditions (Kumar, 2011). The data were collected from the sample and statistically analysed with Microsoft Office Excel 2016 to calculate averages, percentages, and standard deviations to confirm the current applicability of the identified operational risk control measures. Consequently, the researcher complied with the research ethics that are discussed in this chapter. Gatekeeper approval from the participating banks was granted, allowing the researcher access to the banks' employees for data collection.

The next chapter details the analysis of the data received from the questionnaire to serve as a platform for recommendations.

CHAPTER 5: DATA ANALYSIS

5.1. Introduction

Chapter 4 outlines the research methodology and approach used for this study. This chapter will present and interpret the results obtained from the survey.

As stated in Chapter 4, Section 4.2.6.2, the survey involved the distribution of a questionnaire to the three banks that were willing to participate. The envisaged number of participants for the three banks was 78, which were allocated as per department as follows: business management – 15; financial management – 6; risk management – 24; internal audit – 12; compliance management – 6; and other – 15. Only 41 responses were obtained, reflecting a 53% response rate, which is acceptable for this level of statistical analysis (refer to Table 5.1 for the response per department). The questionnaire consisted of four questions that collected biographical information from participants. Furthermore, question five was divided into two sections with 26 Likert scale questions. Section A aimed to confirm the significance of the operational risk control measures, whereas Section B aimed to determine the extent to which each operational risk control measure is currently implemented.

5.2. Biographical Information of the Participants

The data reported in this section were derived from questions 1 to 4 of the questionnaire. The study included 41 participants. To comply with the ethical constraints outlined in Section 4.3 of Chapter 4, the anonymity of the banks and participants was maintained by assigning numbers to the participants. A total of 41 questionnaires were distributed to the participants, and all of them were completed and returned with no errors. This indicates that 100% of the questionnaires were returned and used for this study. The biographical information is shown in Table 5.1 below.

Table 5.1: Biographical information of the participants

Biographic Information	Response Target per Department	Actual Response per Department	%
Department			
Business Management	15	7	17.1
Financial Management	6	2	4.9
Risk Management	24	11	26.8
Internal Audit	12	8	19.5
Compliance Management	6	3	7.3
Other	15	10	24.4

Focus area			
Business/Operations Management		10	24.4
Internal Audit		6	14.6
Risk Management		7	17.1
Compliance Management		7	17.1
Financial Management		4	9.8
Other		7	17.1
Years of experience in risk management			
<1		2	4.9
3-<5		11	26.8
5-<10		11	26.8
>=10		17	41.5
Years of experience with your organisation			
3-<5		3	7.3
5-<10		22	53.7
>=10		16	39.0

Source: Author's own analysis

Table 5.1 shows the departments where the participants were employed, their focus areas, years of experience in risk management, and years of experience in the bank.

5.2.1. Bank departments

This section shows the department in which participants work at the bank. Business management, financial management, risk management, internal audit, compliance management, and others were the six departments specified. The study focused mainly on departments that have an active role in operational risk management at the bank. Table 5.1 shows that 17.1% of the respondents were within the Department of Business Management, 4.9% were from Financial Management, 26.8% were from Risk Management, 19.5% were from Internal Auditing, and 7.3% were from Compliance, while 24.4% were from other departments that were not specified, such as operations and information technology. Therefore, it may be deduced that the information gathered from the survey is appropriate for

this study because most of the respondents were involved in the identified departments involved in risk management.

5.2.2. Focus area

The respondents were obliged to select the departmental core area in which they worked. According to Table 5.1, 24.4% percent of the participants are primarily responsible for the bank's business/operations management, 14.6% are involved in internal audits, 17.1% are responsible for the control of risk management, 17.1% are responsible for compliance, 9.8% are responsible for financial management, and 17.1% oversee other areas such as IT. According to the literature, business management oversees banks' operations, which includes proactive risk detection and management; risk management is responsible for developing and implementing risk management methods and providing risk reports; and internal audits confirm that risk controls are effective. Therefore, at a combined response rate of 56%, the majority of the respondents' focus areas involved risk management. Therefore, based on the information in Table 5.1, it can be accepted that the information is reliable because it was provided by most employees involved in risk management.

5.2.3. Years of experience in risk management

This question sought data on the participants' years of risk management experience. The goal was to guarantee that the respondents' comments on risk management were based on feedback from experienced employees. Their risk management experience was classified as 0-1 year, 1-3 years, 3-5 years, 5-10 years, or more than ten years. According to Table 5.1, 4.9% of participants had less than one year of risk management experience, and 26.8% had three years to five years of experience. Furthermore, 26.8% of the participants had less than 10 years of risk management experience, while the remaining 39.00% had more than 10 years of experience. Based on the responses, 65.8% of the respondents had more than 5 years of experience in risk management, and it can be accepted that their responses to the survey reflected realistic and true results.

5.2.4. Years of experience with your organisation

Table 5.1 shows the participants' years of experience in their current workplace. According to the responses, 7.3% had between 3 and 5 years of experience with their current organisation, 53.7% had more than 10 years of experience, and 39.0% had less than 10 years of experience. Thus, the results of the survey illustrate a realistic reflection in terms of the respondents' years of employment with their relevant organisations. As such, it can be accepted that most participants should have a high level of exposure to the understanding and implementation of risk management in their respective banks and that their response could add value to the findings of the survey.

5.3. Results Interpretation

This section summarises the results of Question 5, which was divided into two sections. Section A prompted participants to indicate how much they agreed or disagreed that risk controls are important, and Section B asked them to indicate how much they agreed or disagreed that the control measures were applicable in their organisation. The 26 sub questions emanate from the conclusions reached in Chapters 2 and 3 concerning operational risk control measures for a bank during a crisis. The t-test statistic was used, and as indicated in Section 4.9.1.5, it is a type of statistical analysis used to compare the averages of two groups or two sets and determine whether there is a difference between means (De Villis, 2011). In this study, the means of importance of a risk control measure are compared with those of its applicability to determine the gap between two variables while still using the same respondents (De Villis, 2011). Furthermore, the standard deviation was additionally determined to reflect how the data were distributed around the mean, and the significance level of the two means was ultimately measured to determine whether there was any statistical evidence that the two means were different. The study measured the p value against 95% confidence, 0.05 significance level, whereby $P \leq 0.05$ means there is significant evidence that the two means are different. The findings are shown in Table 5.2 below.

Table 5.2: Independent sample t-test for the equality of means

	Group	Mean	Std. Deviation	Significance
Q1	Importance	4.93	.346	.000
	Current applicability	3.66	.693	
Q2	Importance	4.71	.901	.000
	Current applicability	3.80	1.054	
Q3	Importance	4.83	.381	.000
	Current applicability	3.59	.741	
Q4	Importance	4.78	.759	.000
	Current applicability	3.98	.935	
Q5	Importance	4.80	.459	.001
	Current applicability	4.37	.662	
Q6	Importance	4.90	.374	.001

	Current applicability	4.54	.596	
Q7	Importance	4.98	.156	.000
	Current applicability	4.51	.553	
Q8	Importance	4.88	.640	.002
	Current applicability	4.37	.799	
Q9	Importance	4.90	.300	.000
	Applicability	4.37	.767	
Q10	Importance	4.95	.218	.000
	Current applicability	4.05	.773	
Q11	Importance	4.80	.459	.000
	Current applicability	4.24	.830	
Q12	Importance	4.90	.300	.000
	Current applicability	3.88	.842	
Q13	Importance	4.93	.264	.000
	Current applicability	4.02	.790	
Q14	Importance	4.93	.346	.000
	Current applicability	4.29	.680	
Q15	Importance	4.90	.300	.000
	Current applicability	3.76	.767	
Q16	Importance	4.78	.690	.004
	Current applicability	4.22	.988	
Q17	Importance	4.78	.759	.001
	Current applicability	4.05	1.071	
Q18	Importance	4.88	.557	.003

	Current applicability	4.56	.673	
Q19	Importance	4.93	.346	.000
	Current applicability	4.34	.530	
Q20	Importance	4.98	.156	.000
	Current applicability	4.51	.597	
Q21	Importance	4.83	.381	.000
	Current applicability	4.12	.781	
Q22	Importance	4.93	.264	.000
	Current applicability	4.20	.843	
Q23	Importance	4.90	.300	.000
	Current applicability	3.90	.860	
Q24	Importance	4.95	.218	.000
	Current applicability	4.00	1.025	
Q25	Importance	4.93	.264	.000
	Current applicability	4.22	1.129	
Q26	Importance	4.88	.510	.000
	Current applicability	3.83	1.070	

Source: Author's own analysis

Question1. Operational risk should be clearly defined and understood by all employees of the bank, and the responses are presented in Figure 5.1.

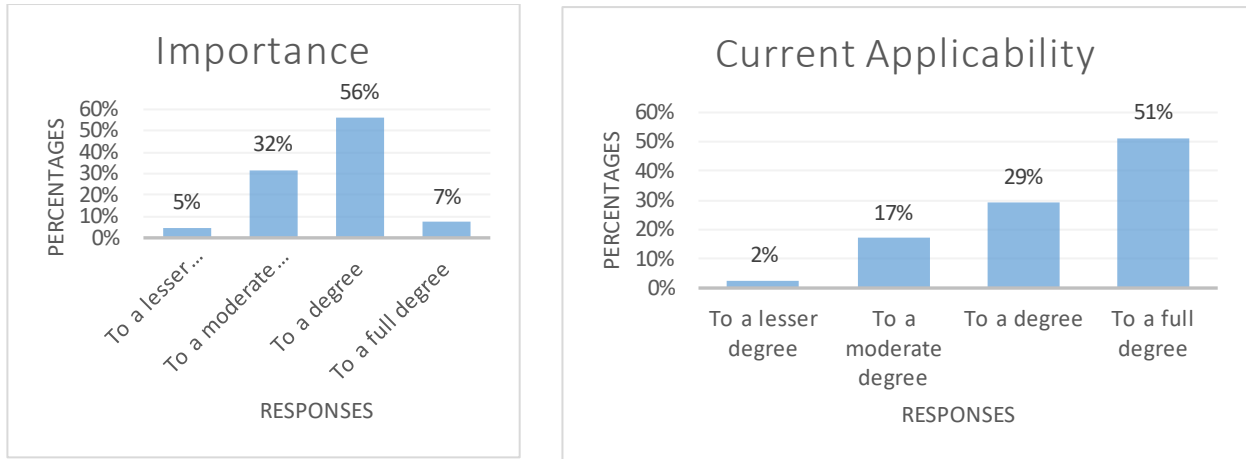


Figure 5.1: Definition of operational risk management

Source: Author's own analysis

According to the responses, 63% of participants indicated to a degree and to a full degree that it is critical for a bank to properly define operational risk and ensure that all employees understand it, while 37% agreed to a lesser or moderate degree. In terms of the current implementation, 80% of the participants agreed, to a degree and to a full degree, that operational risk is defined and understood by employees in their respective banks. According to Table 5.2, the mean degree of importance for this control measure is 4.93, which is higher than the mean of the existing applicability, which is 3.66. The importance standard deviation is 0.346, while the current applicability standard deviation is 0.693, indicating that respondents' views on the importance of a clear definition of operational risk within banks were closer to the mean than the current applicability of this risk control measure. This suggests that most of the respondents agree with the need for a bank to have a clear definition of operational risk compared to its current application. Additionally, the p-value of 0.000, which is less than 0.05, implies that there is significant evidence that the means of importance of a clear explanation of operational risk to be understood by all employees and its applicability are not different.

The results of a descriptive analysis identified a gap in the current applicability based on the means, with a variance of 1.27 from the importance. This illustrates that although banks regard a clear definition of operational risk as important and have implemented it, the control measure is deemed more important than is currently applicable. According to the literature, banks should clearly define operational risk to ensure that it is understood by all employees and to enable employees to identify specific risk factors that a crisis event could expose banks to, allowing the bank to be proactive in managing those risk factors. Therefore, it can be concluded that a clear definition of operational risk can help a bank meet its objective of effective operational risk management and be proactive in preparing for possible crisis events.

Question 2: An operational risk management framework should be embedded to serve as a platform to guide effective operational risk management. This question indicates that for effective operational risk control, banks need to embed an operational risk management framework. The responses are shown in Figure 5.2.

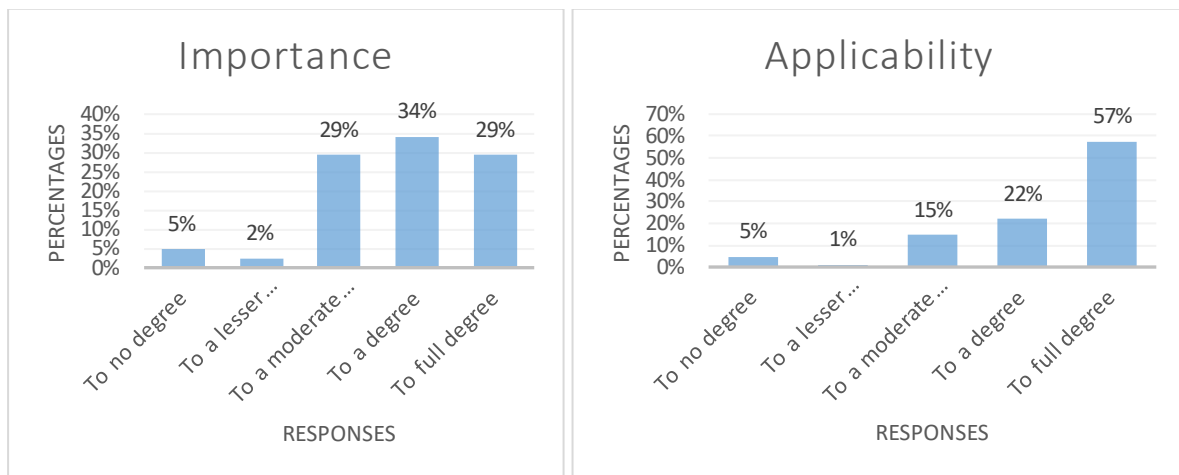


Figure 5.2: Operational risk management framework

Source: Author's own analysis

Figure 5.2 shows that 63% of participants agreed to a degree or full degree that a bank should establish an operational risk management framework to provide guidance toward effective operational risk management. According to 31% of the participants, an operational risk management framework is important, but to a lesser and moderate degree, 5% disagree. The current applicability of this control measure is 79%, while 16% of respondents rated it as applicable, albeit to a lesser or moderate degree. Five percent of participants stated that banks do not have operational risk management frameworks in place to effectively manage operational risk. According to the feedback, most respondents regarded the embedding of a risk management framework as an important risk control measure, while the current rating of applicability was confirmed by 79%. The t-test for the equality of means revealed that the mean degree of importance for a bank to embed a risk management framework is 4.71, which is greater than the mean existing applicability of 3.80. The standard deviation for importance is 0.901, while the standard deviation for current applicability is 1.054, indicating that the data for respondents' views on the importance of embedding a risk management framework were closer to the mean than the data for respondents' views on the current applicability. According to Table 5.2, the p-value is 0.000, which is less than 0.05, indicating significant evidence that the mean importance of having a risk management framework embedded and its existing applicability are not different. The results of the descriptive analysis identified a gap in the current applicability based on the means, with a variance of 0.91 from the importance. This

illustrates that operational risk management frameworks form an important risk control measure and that most banks have embedded a framework within their respective banks. As such, the control measure has been implemented in most banks. However, it seems, based on the variance, that although embedding a risk management framework is deemed important, it has not been equally adopted by banks. According to the literature, for effective risk management, an organisation needs to develop and implement a risk management framework that will provide guidance and support towards achieving the objective of effectively managing risks. The embedding of an operational risk management framework is an important risk control measure. According to the response, although a risk management framework is regarded as important, not all banks have adopted this control measure. Therefore, it is concluded that banks should embed a risk management framework to serve as a platform for effective risk management.

Question 3. A risk culture should ensure the embedding of norms, attitudes and behaviours of employees relating to risk controls. Figure 5.3 demonstrates the response to the importance of risk culture to ensure embedded norms, attitudes and behaviours that relate to operational risk control and its current applicability within banks.

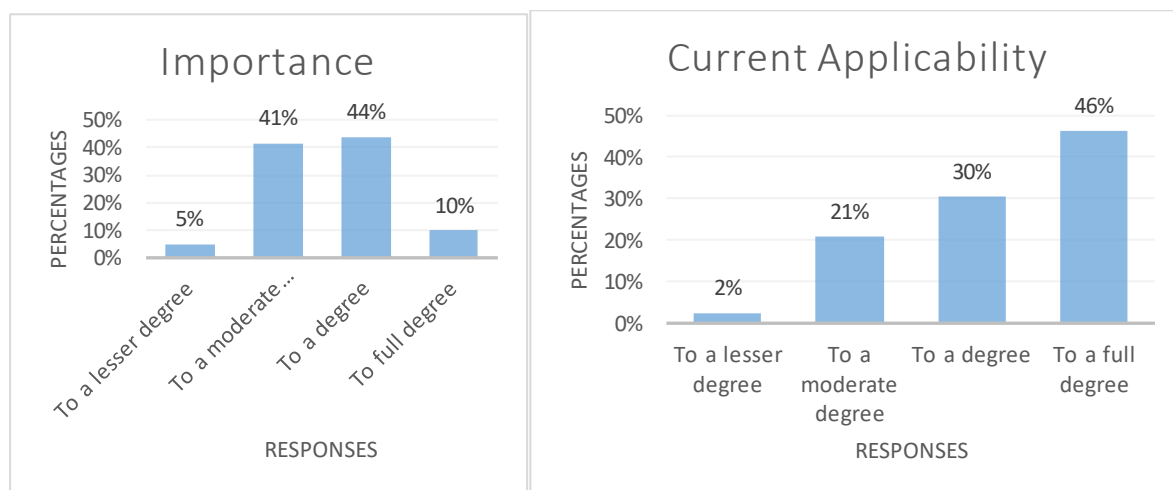


Figure 5.3: Risk culture

Source: Author's own analysis

Based on the feedback, 54% of participants indicated to a degree and to a full degree that it is important for banks to have a culture that ensures the embedding of norms, attitudes, and behaviours relating to risk culture as a risk control measure. Figure 5.3 also shows that 46% of participants agree, but to a lesser or moderate degree, that it is important to have a risk culture that ensures the embedding of norms, attitudes, and behaviours that are related to risk control. The current applicability of this control measure is 76%, while 23% of the data are applicable, although to a lesser or moderate degree. Based on the significance rating of 54%

and the current applicability of 76% for embedding risk culture as a control measure, it seems that although risk culture is embedded in most banks, its importance is unclear. According to the t-test for the equality of means to compare the importance of embedding a risk management culture that relates to risk controls and its applicability, the mean importance of embedding a risk management culture is 4.83, which is greater than the mean for an existing applicability of 3.59. The standard deviation for the significance of embedding a risk culture that relates to risk control is 0.381, while the standard deviation for its applicability is 0.741. This indicates that the data on respondents' views regarding the substance of having risk management embedded were closer to the mean than the data on respondents' views on the existing applicability of risk management. This shows that most of the respondents agree with the need for a bank to have a risk culture that embeds the norms, attitudes and behaviours that relate to risk control compared to its current applicability. The p-value is 0.000, which is less than 0.05, indicating sufficient evidence that the means of importance for ensuring the embedding of norms, attitudes and behaviours related to risk control and its applicability are not different. The results of a descriptive analysis identified a gap in the current applicability based on the means, with a variance of 1.24. This indicates that respondents regard the embedding of a risk culture that embeds the norms, attitudes and behaviours that relate to risk control as important. However, there seems to be a gap in the applicability of this control measure. According to the literature, a bank needs to ensure the implementation of a risk culture that embeds the norms, attitudes and behaviours that will lead a bank towards effective control of the risks to which the bank may be exposed. Therefore, this control measure is important for achieving the goal of effective risk management and proactively preparing for a crisis. Hence, banks need to implement this approach.

Question 4. A risk management strategy should be aligned with the business strategy to ensure that the objectives are within the set parameters of the risk appetite. The results of the participants' ratings regarding aligning the risk management strategy with the overall strategy of the bank and the level of current applicability are illustrated in Figure 5.4 below.

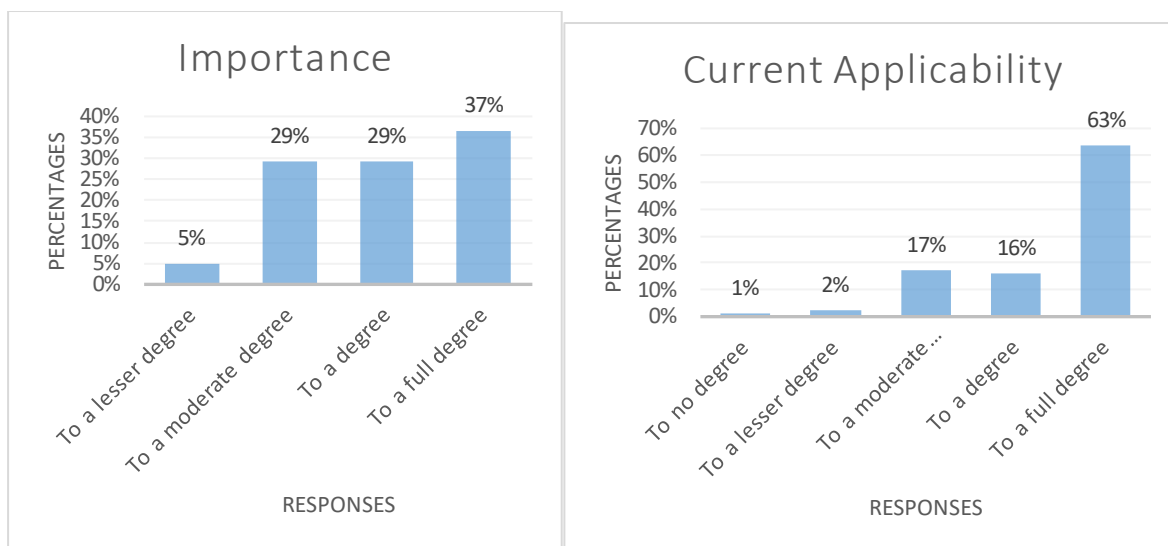


Figure 5.4: Risk management strategy

Source: Author's own analysis

Figure 5.4 shows that 66% of participants agree, to a degree and to a full degree, that it is important to align the risk management strategy with the business strategy of the bank to guarantee that the goals are achieved within the allocated limits of the bank's risk appetite. According to 34% of participants, aligning risk management strategies with business strategies is important but to a lesser or moderate degree. According to the findings, the current applicability of this control measure is rated at 82%, while 5% of the participants rated it as applicable but to a lesser or moderate degree. According to 1% of participants, banks have not aligned their risk management strategies with their overall business strategy.

According to the t-test, the mean of the participants' views on the importance of a bank aligning its risk management strategy with its business strategy to guarantee that the objectives are within the usual limits of risk appetite is 4.78, which is higher than the mean of their views on current applicability, which is 3.98. Furthermore, the standard deviation for importance is 0.759, and the standard deviation for current applicability is 0.935, indicating that the data for the respondents' views on the substance of aligning a risk management strategy with the business strategy are closer to the mean than the data for respondents' views on the existing applicability. This indicates that most of the respondents agree with the need for banks to align their risk management strategies with their business strategies to ensure that the objectives remain within the set limits of their risk appetite. Nonetheless, the p-value is 0.000, as shown in Table 5.2, confirming that there is sufficient evidence that the means of importance of aligning risk management strategies with business strategies and of existing applicability are not different. The results of a descriptive analysis identified a gap in the current applicability based on the means, with a variance of 0.8. This illustrates that, according to respondents,

aligning risk management strategies with business strategies is important. However, the control measure is not being applied as much as it is deemed important.

The variance could indicate that this control measure is embedded only in top management and that not all employees are involved or knowledgeable about the importance of this control measure for operational risk. In addition, this could also lead to an unclear risk appetite at an operational level, which could negatively influence the achievement of business objectives. Thus, it is concluded that banks should safeguard against aligning risk management strategies and business strategies and that all employees are aware of the resultant risk appetite, which is an important guideline for operations, including being prepared for potential crisis events. In addition, it is important that all involved parties be trained and knowledgeable on the concept of an operational risk appetite and are aware of the contributions it can make to proactively managing a crisis event.

Question 5: A governance structure should be embedded to confirm the roles and responsibilities of role-players in risk management. Figure 5.5 shows the participants' ratings of the importance of a bank to embed a governance structure to confirm the roles and responsibilities of the role of players in risk management.

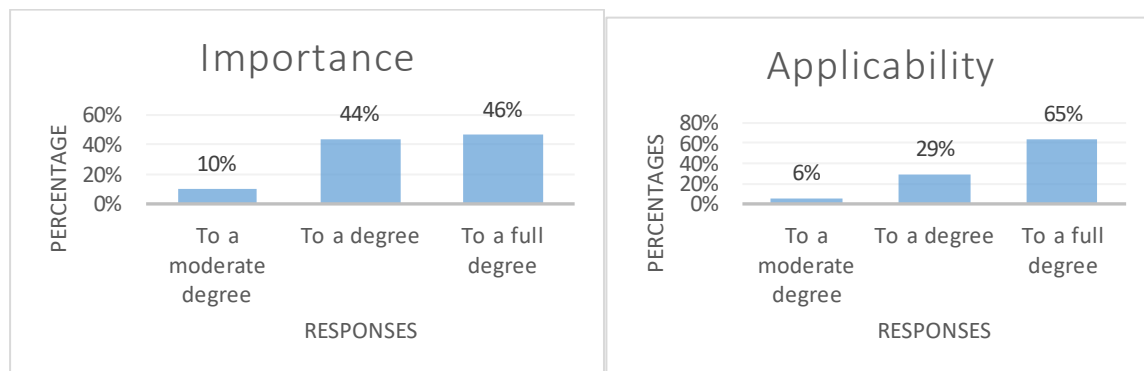


Figure 5.5: Governance structure

Source: Author's own analysis

Figure 5.5 shows that 90% of participants agreed that a bank should embed a governance structure to confirm the roles and responsibilities of role players in risk management. According to 10% of participants, governance structure is important but to a moderate degree. The current applicability of this control measure is indicated by 94% of participants who agreed that there is a risk governance structure in place, while 6% of participants agreed that it is applicable but to a moderate degree. Based on the t-test, the mean of the participants' views on the importance of the bank embedding governance structure for confirming the roles and responsibilities of role players in risk management is 4.80, which is higher than the mean of

their views on current applicability, which is 4.37. This demonstrates that while most participants agree that having a governance structure incorporated to confirm the roles and duties of role-players in risk management is essential, its current application is not directly proportional to its importance, as evidenced by a variance of 0.43 identified by a descriptive analysis.

The standard deviation for importance is 0.459, which is less than the standard deviation for current applicability, which is 0.662. This implies that the data on participant views regarding the importance of banks having an embedded governance structure were closer to the mean than the data on their views on current applicability. However, the p-value is 0.001, which indicates that there is sufficient evidence that the mean of importance of embedding a governance structure to confirm the roles and responsibilities of role players in risk management and the mean of its applicability are not different. Therefore, most participants regarded embedding a risk governance structure and the related roles and responsibilities of role players in risk management as important operational risk control measures. In addition, it seems that most banks have embedded a risk governance structure as a risk control measure. The literature reveals that embedding a governance structure that confirms the roles and responsibilities of role players in risk management is an important tool that contributes to the effective risk management of banks. It is evident that embedding a governance structure is important. However, although governance structures have been embedded, it remains imperative that governance structures be adapted to a changing environment, especially in view of the latest global events such as the COVID-19 pandemic, to ensure that a bank is prepared for such events and that all role-players are aware of their roles and responsibilities. Therefore, for example, it is crucial that regular testing of business continuity plans take place to guarantee an acceptable state of preparedness for crisis events.

Question 6. A risk management process should be formalised and embedded in the organisation. This question implies that a bank needs to have a formal risk management process embedded. The results are illustrated in Figure 5.6 below.

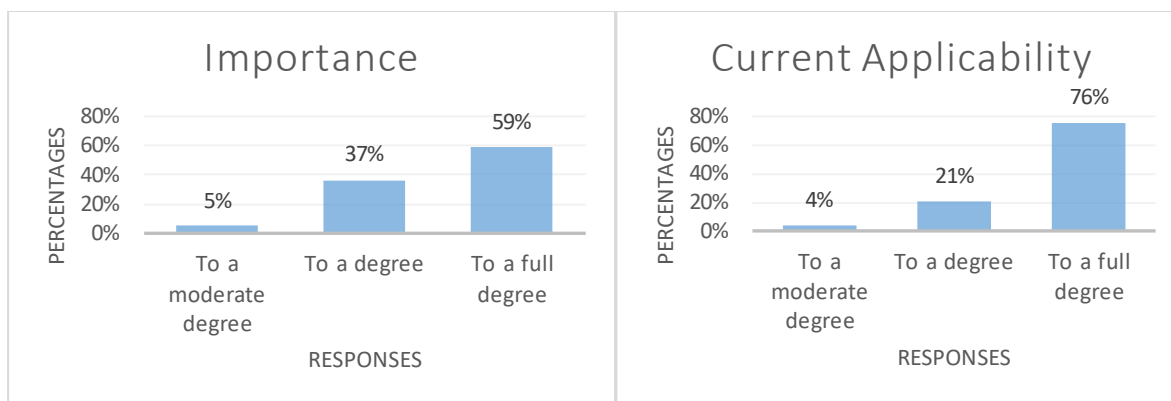


Figure 5.6: Risk management process

Source: Author's own analysis

The results in Figure 5.6 show that 96% of participants agree to a degree and to a full degree that it is important for a bank to have a formalised risk management process that is embedded within the bank as a risk control measure. The current applicability of this control measure is 97%. The t-test for the equality of means was used to compare the significance of having a formalised risk management process embedded within the bank as a risk control measure and the applicability of this control measure. The results, as shown in Table 5.2, indicate that the mean importance of having a risk management process embedded as a control measure is 4.90, while the mean current applicability is 4.54. Furthermore, the standard deviation of the importance of embedding a risk management process is 0.374, which is smaller than the applicability rating of 0.596, which indicates that data for importance were closer to its mean than data for applicability. Therefore, most respondents shared the view that the importance of improving the risk management process outweighs its current applicability. Additionally, the p-value is 0.000, which is less than 0.05, indicating that there is significant evidence that the mean of the importance of embedding a risk management process within the bank to proactively manage operational risk during a crisis and that of the current applicability are not different. The results of the descriptive analysis identified a gap in the current applicability of the scale, based on a significance level of 0.36. This illustrates that although banks see the embedding of a formalised risk management process as important and have implemented it, the risk control measure is deemed more important than is currently applicable. According to the literature, organisations should outline their risk management process and embed it within the organisation. According to the respondents, the high degree of importance and current applicability of risk management illustrate that an embedded risk management process is a crucial risk control measure. Therefore, an embedded risk management process can assist a bank in achieving its objectives and proactively prepare for possible crisis events.

Question 7: Risk identification should constitute a step of an operational risk management process to identify inherent risk exposures. This question suggests that risk identification should be incorporated as a step of an operational risk management process. Figure 5.7 shows the results.

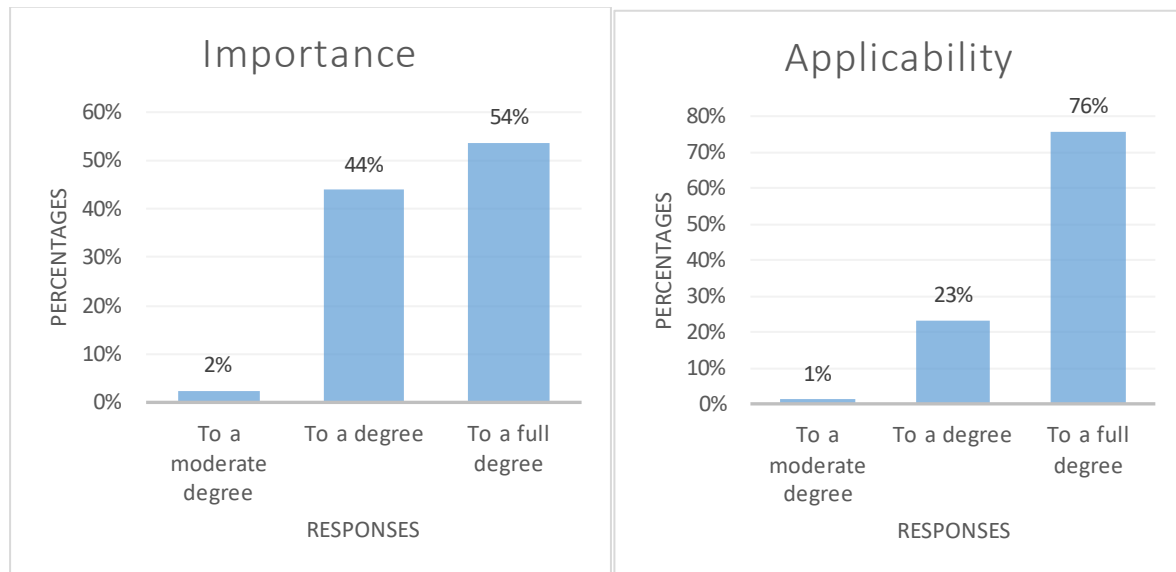


Figure 5.7: Risk identification

Source: Author's own analysis

A literature review revealed that risk identification is a step in the risk management process that assists banks in identifying inherent risks. Therefore, banks need to incorporate risk identification as a step in their risk management process. According to Figure 5.7, 98% of participants agreed to a degree and to a full degree that it is important for risk identification to be included as a step in the risk management process of the bank to assist the bank in achieving the objective of effective risk management. According to 99% of participants, banks have included risk identification as a step in their risk management process. Based on the results of the t-test, the mean of the participants' views on the importance of risk identification as a step in an operational risk management process to identify inherent risk exposures is 4.98, which is higher than the mean of their views on present applicability, which is 4.51. This suggests that most respondents contend that having a risk identification process, as a phase in an operational risk management process, is necessary for identifying inherent risk exposures. However, the current applicability is not directly proportional to importance.

According to Table 5.2, the respondents' views on the importance of including risk identification as a step in the risk management process were closer to their mean than their views on the current applicability. However, the p-value is 0.000, demonstrating sufficient evidence that the importance of including risk identification in the risk management process

and its applicability are not different. As such, it is evident that risk identification is an important step in a risk management process that will assist employees in identifying the risk exposures to which they could be exposed to effectively manage the risks. In conclusion, this is an important risk control measure for identifying risks to achieve business objectives and prepare for potential crisis events. Thus, it must be a step in a risk management process.

Question 8: Risk evaluation should be a step of an operational risk management process to assess the identified risks in terms of likelihood and impact. The literature reveals that banks need to evaluate the identified risks to determine the potential impact and likelihood of proactively identifying and allocating appropriate control measures. The response to this question is shown in Figure 5.8.

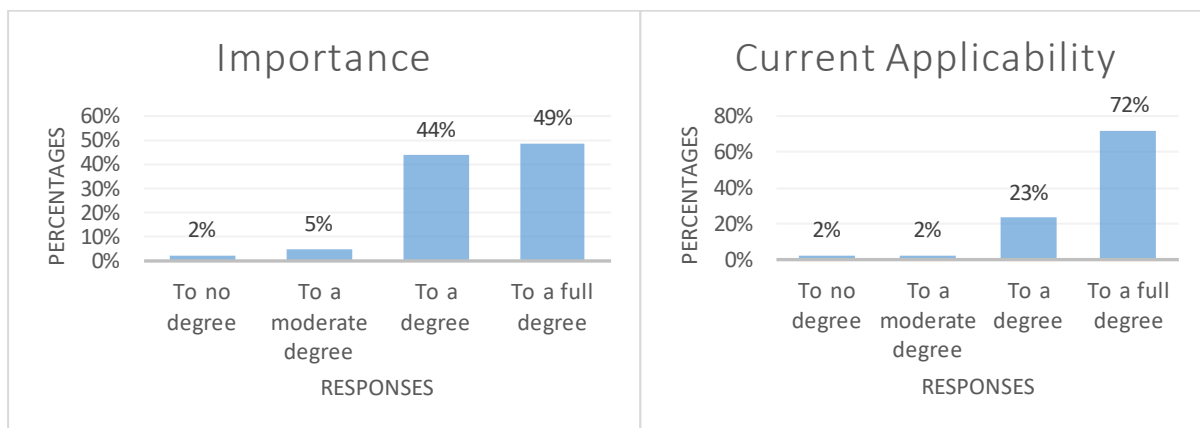


Figure 5.8: Risk evaluation

Source: Author's own analysis

Figure 5.8 shows that 93% of participants rated to a degree and to a full degree that risk evaluation should be another step in the risk management process. According to the responses, 95% of the respondents agreed to a degree or a full degree that risk evaluation is applicable as a step in the risk management process and therefore part of a risk control measure. Furthermore, the mean of participants' opinions on the importance of risk evaluation as a step in an operational risk management process to analyse the recognised risks in terms of likelihood and impact is 4.88, which is higher than the mean of their opinions on current applicability, which is 4.37. According to Table 5.2, the data for participants' views on the current applicability were more evenly distributed around the mean than the data for their views on its importance. This is explained by the fact that the standard deviation of importance is 0.640, which is less than the standard deviation of the current applicability, which is 0.799. The results of the descriptive analysis identified a gap in the current applicability of the scale, based on a significance level of 0.51. This indicates that most of the participants agreed that risk evaluation is an important step in an operational risk management process to assess the

identified risks in terms of likelihood and impact. However, risk control measures are not implemented as much as they are deemed important. On the other hand, Table 5.2 also shows that the p-value is 0.002, which indicates that there is sufficient evidence that the mean of the importance of incorporating risk evaluation into a risk management process and the mean of the risk control application are not different. According to the literature, risk evaluation as a step in a risk management process will assist banks in evaluating the identified risks to determine the potential impact and likelihood of the risks. Therefore, it is determined that risk evaluation is another critical step of a risk management process as a control measure for banks to guarantee the bank's objective of effective operational risk management and to prepare for potential crisis events, as it can also be regarded as providing a platform for the formulation of risk control and mitigation measures.

Question 9: Risk control and mitigation should constitute a step of an operational risk management process to establish risk control measures for the identified risks. As indicated in Section 2.7 of Chapter 2, risk control and mitigation should be included in an operational risk management process to enable banks to develop risk controls and mitigations for the identified and evaluated risks. The results are represented in Figure 5.9 below.

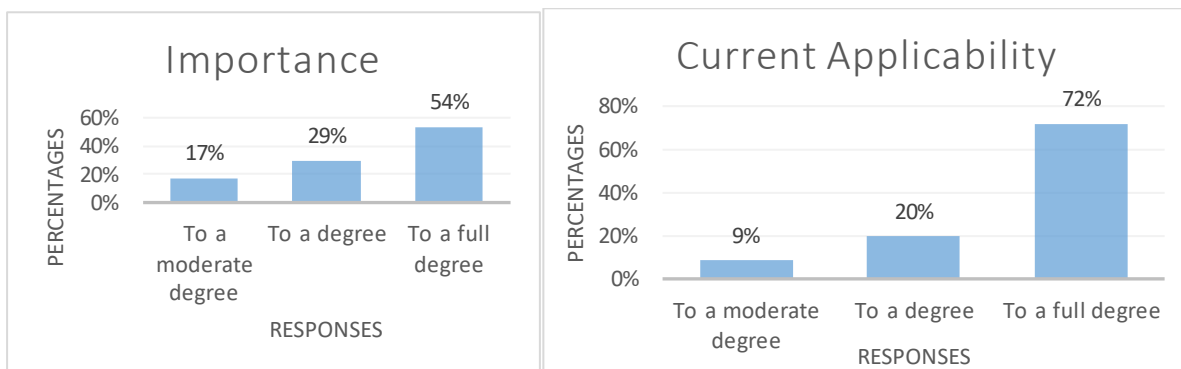


Figure 5.9 Risk control and mitigation

Source: Author's own analysis

Figure 5.9 indicates that 83% of participants agreed to a degree and to a full degree that risk control and mitigation should be a step of an operational risk management process to establish risk control measures for the identified risks. According to 17% of participants, risk control and mitigation should be a step in the operational risk management process; however, to a moderate degree. Based on the responses, 92% of participants agreed to a degree and to a full degree that this control measure is currently applicable in banks. A t-test was computed to compare the means of responses on the importance of including risk control as a step in the risk management process and the mean of its implementation. According to the results, the mean of respondents' opinion regarding the importance of risk control and mitigation as a step

in an operational risk management process for establishing risk control measures for the identified risks is 4.90, which is higher than the mean of their views on current applicability, which is 4.37.

Furthermore, the data for participants' opinions on the significance of including risk control and mitigation as a stage of a risk management process were closer to the mean than were the data for participants' views on its current applicability. This is indicated by a standard deviation of importance of 0.30, which is less than the standard deviation of the mean of 7.67 for current applicability. This indicates that most respondents had a more common view of the importance of this control measure than its current applicability. This was also demonstrated by the 0.53 identified as a gap in the means of current applicability and importance based on the descriptive analysis. However, Table 5.2 shows that the p value of this control measure is 0.000, which is less than 0.05; therefore, there is significant evidence that the mean of the importance of including risk control as a step of a risk management process and the mean of its implementation are not different. The literature confirms that risk control and mitigation are important steps in a risk management process that aims to enable banks to develop risk controls and mitigate identified and evaluated risks.

Moreover, most participants indicated that banks currently incorporate risk control and mitigation into their risk management process. However, the variance of 0.53 between the mean of the importance and the applicability of this step seems to indicate that although risk control measures may be considered an important step in operational risk management risk control, the applicability of these measures may be underestimated. According to the literature, business continuity management is an important operational risk control method. As such, BCM is a result of the risk control and mitigation steps of a risk management process. Therefore, it is imperative that this step be implemented in a bank's risk management process, which could lead to effective crisis management. This can be achieved through awareness training for all employees regarding risk control and mitigation measures to prepare for risk exposures and potential crisis events.

Question 10: Risk monitoring should constitute a step of an operational risk management process to ensure the continuous monitoring and reporting of risks and control measures. This question implies that banks need to continuously monitor risk controls to ensure that they remain effective. The results are shown in Figure 5.10 below.

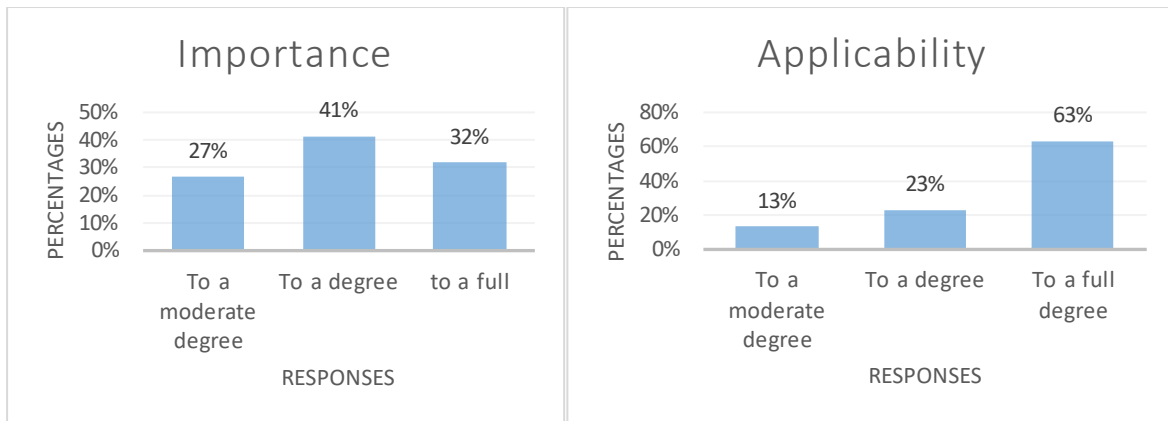


Figure 5.10: Risk monitoring

Source: Author's own analysis

Figure 5.10 demonstrates that 73% of participants agree to a degree or full degree that risk monitoring should be incorporated into the risk management process of the bank to allow continuous monitoring of the risk controls and ensure that they are still effective. According to 27% of participants, risk monitoring is important but to a moderate degree. The current applicability of this control measure is 86%, while 13% of the participants rated it as applicable, although to a moderate degree. The mean of the views on importance is 4.95, which is higher than the mean of the views on current applicability, which is 4.05. This figure depicts a variance of 0.90 between the mean of the importance of including risk monitoring in the risk management process and its implementation. The variance could imply that although most respondents agree that this risk control measure is important, it is not implemented by some banks. Additionally, the standard deviation for the importance of this control measure is 0.218, which is less than the standard deviation of applicability.

These findings demonstrate that the data on the views of respondents on the importance of including risk monitoring as a step in the risk management process were closer to its mean than the data on the views of the implementation of this control measure. According to the literature, banks need to continuously monitor their risk controls to ensure that they remain effective. As such, the majority of participants regard risk monitoring as an important risk control measure that is implemented by most banks. This was confirmed by a p-value of 0.000, which is less than 0.05. However, the variance of 0.90 could indicate that although most banks understand the importance of risk monitoring in the risk management process, risk monitoring may not be implemented adequately for some banks. This can also be substantiated by the 13% of respondents who rated this control measure as applicable to a moderate degree. Another reason for the lower rating of the applicability of this control measure can be attributed to the possibility that risk monitoring is not adequately performed by all role-players. In

conclusion, the risk monitoring step as part of the risk management process must be specifically addressed in policy documents to specify the roles and responsibilities of all role-players. This approach could ensure that risk monitoring can proactively detect loopholes in risk control measures, which can be rectified.

Question 11. Organisations should appoint employees who are responsible for identified critical functions during a crisis event. The literature further reveals that a bank needs to identify employees who will continue critical operations during a crisis (refer to Chapter 3, Section 3.5, bullet 7, sub bullet 1). The responses are shown in Figure 5.11 below.

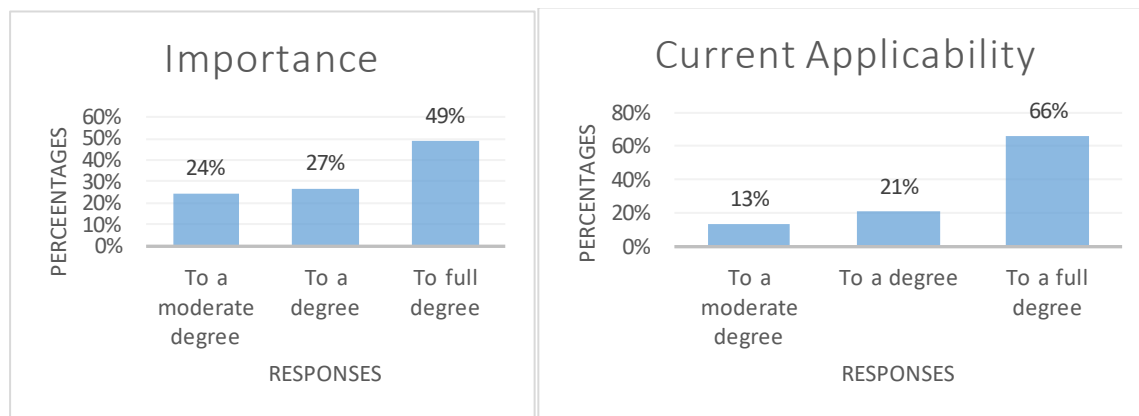


Figure 5.11: Appointing employees for critical functions

Source: Author's own analysis

Figure 5.11 demonstrates that 76% of participants agree to a degree that banks should appoint employees who will continue the identified critical functions within the bank that must remain operational even during a crisis event. According to 24% of participants, appointing employees is important, although to a moderate degree. Based on a rating of 87%, this control measure is currently adopted by most banks; however, 13% of participants indicated that critical employees have been appointed only to a certain extent. According to the t-test results, the mean of the participants' views on the importance of organisations selecting employees who are responsible for established critical functions during a crisis event is 4.80, which is higher than the mean of their views on its applicability, which is 4.24. This depicts a gap of 0.56 in the current applicability based on the means of importance and could imply that the majority of respondents believe it is important for organisations to select employees responsible for the identified critical functions during times of crisis; it also suggests that the control measure is not implemented as much as it is deemed important. Furthermore, the standard deviation of this control measure's level of importance is 0.459, while the current applicability is 0.0830, which is greater. This indicates that the data for the respondents' opinions on the importance of the bank in identifying critical employees who will continue critical operations of the bank

during a crisis were closer to its mean than the data for the participants' views on the implementation of this control measure. The statistical evidence demonstrates that the mean for the importance of identifying critical employees and the mean for its applicability are not different. The results were confirmed by a p value of 0.000, which is less than 0.05. According to the literature, banking is an essential service, and it must remain operational during a crisis. Therefore, it is critical for banks to identify employees who will carry out critical bank operations. According to the responses, this operational risk control is important. Therefore, identifying employees who perform critical control measures to prepare a bank for a crisis event is an important risk control measure. However, the 0.56 gap identified could suggest that although most banks understand the importance of having dedicated employees who will perform critical functions of the bank in case of a crisis, some banks are still not adequately prepared in this regard. Therefore, banks should improve their crisis preparedness by ensuring that there is enough personnel to carry them through a crisis of any kind. Adequate allocation of resources is critical for implementing this operational risk control measure, and it is imperative that these allocated responsibilities be included in job descriptions.

Question 12: Employees should be trained to understand and perform their functions during a crisis event. This question implies that although a bank has identified employees, these employees must be trained to understand their functions during a crisis event (Chapter 3, Section 3.5, bullet 7, and sub bullet 2). The responses are shown in Figure 5.12 below.

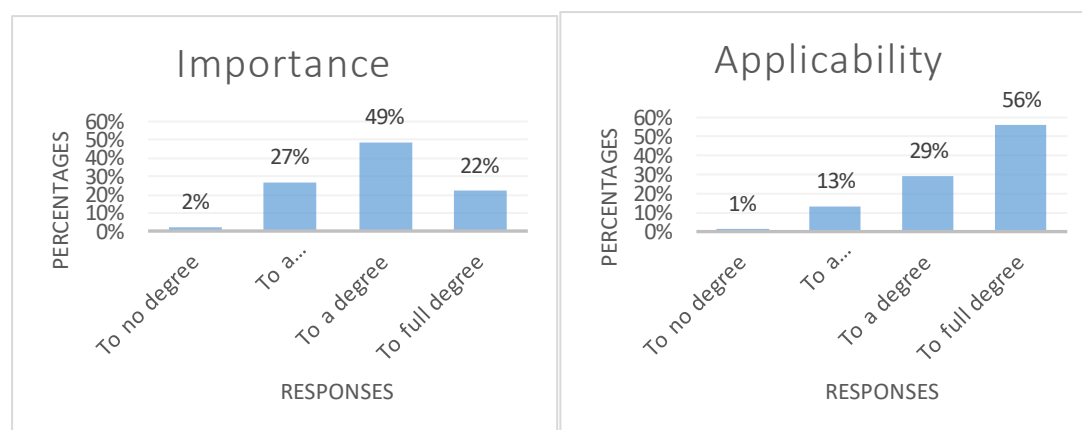


Figure 5.12: Training of employees

Source: Author's own analysis

According to Figure 5.12, 71% of participants agreed to a degree or full degree that training employees is critical to ensuring that they understand their roles and what they are expected to do during a crisis. Nonetheless, 27% of participants agreed to a moderate degree that training is important for employees, while 2% indicated that this control measure is not important. According to 85% of participants, banks have provided sufficient training to

employees, suggesting that critical employees understand their roles and are ready to continue operations during a crisis. However, some employees question their readiness to continue with the bank's critical operations when a crisis occurs. A comparison of participants' perspectives on the importance and applicability of this control was computed. The corresponding means were 4.80 and 3.88, respectively. This indicates a gap of 0.92 between the mean importance of the control measure and its importance, which could suggest that the majority of participants rated that it is essential for employees to be trained to understand and fulfil their functions during a crisis event, although the risk control measure may not be applicable in some banks.

Additionally, the data on participants' views on the importance of training employees were closer to the mean than the data on their views on applicability were. This is explained by the fact that the standard deviation of importance is 0.300, which is less than the standard deviation of the current applicability, which is 0.842. However, the p-value in Table 5.2 is 0.000, indicating that there is substantial evidence that the mean importance of training critical staff and the mean applicability are not different. A crisis event could entail a change in the normal working environment. For example, remote working is highlighted in the literature review because it entails engaging differently with customers and adopting new ways to carry out duties. Therefore, it can be concluded that it is important for banks to train their employees as a proactive control measure in a crisis. This approach ensures that all employees responsible for tasks during a crisis understand their roles and responsibilities. For example, it is imperative for banks to perform drills to test their business continuity plans to implement this control measure.

Question 13: Organisations should ensure a healthy and safe environment for employees during times of crisis. Based on the conclusions drawn from the literature review, it is important that employees who perform critical functions of a bank during a crisis remain healthy and safe (refer to Chapters 2 and 3). Figure 5.13 below illustrates the results.

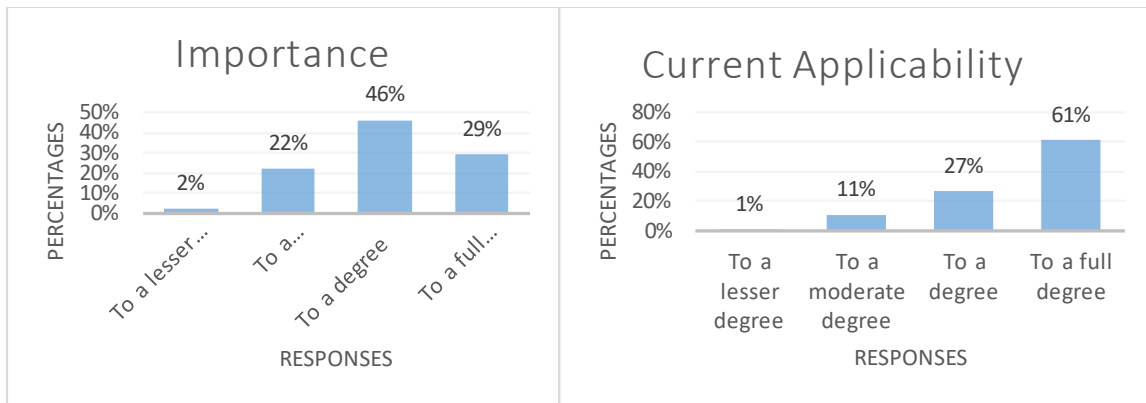


Figure 5.13: Health and safety environment

Source: Author's own analysis

Figure 5.13 shows that 75% of participants agreed that ensuring a healthy and safe environment is important for employees during a crisis event. According to 24% of the responses, a healthy and safe environment is important but to a lesser and moderate degree, respectively. The current applicability of this control measure is 88%, while 12% of participants rated it as applicable but to a lesser and moderate degree. According to Table 5.2, the mean importance of organisations creating a healthy and safe environment for employees during times of crisis is 4.93, which is greater than the mean of their position on their current application, which is 4.02. Furthermore, the standard deviation of importance is 0.264, which is lower than the standard deviation of the current applicability, which is 0.790. Nonetheless, the p-value is 0.000, which is less than 0.05. Therefore, these results show a gap of 0.91 between the mean for importance for banks to ensure a healthy and safe working environment for employees and the mean for applicability of this control measure. This could suggest that although most participants agree that it is critical for organisations to provide a safe environment for employees during times of crisis, there is still a lack of such an environment as far as implementation is concerned.

Additionally, the standard deviations indicate that the data from the participants' views on the importance of this control measure were closer to the mean than were those from its applicability. However, the p-value of 0.000 indicates that the means of the importance for having a healthy and safe environment and its applicability are not different. As such, most of the participants regard ensuring that employees remain safe and healthy during a crisis event as an important risk control measure that is implemented by most banks. According to the literature, the banking industry is essential and ought to remain operational during a crisis. This exposes employees of the bank to a possible health and safety risk that may result from a crisis. Therefore, although employees must work under potentially unsafe conditions, such as those experienced during the COVID-19 pandemic, they should be provided with all

necessary resources, depending on the event, to secure their health and safety. Additionally, safety drills and procedures for how employees should protect themselves during a crisis event are among the measures a bank could provide to its employees to ensure the objective of effective proactiveness and crisis preparedness.

Question 14. Organisations should develop adequate policies and procedures to ensure the continued operation of business processes during times of crisis. The literature review revealed that organisations need to have adequate policies and procedures in place to allow for business continuity during a crisis event (refer to Chapters 2 and 3). The results are shown in Figure 5.14 below.

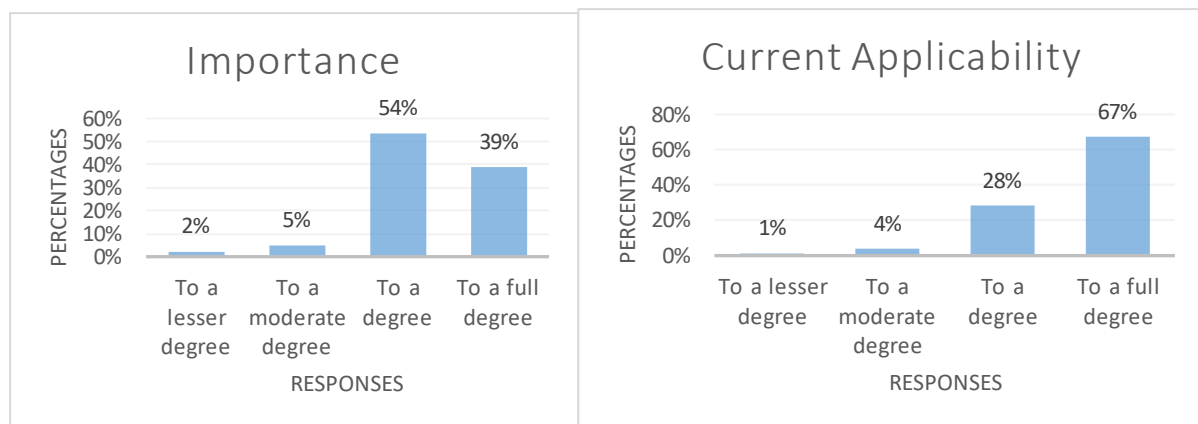


Figure 5.14: Policies and procedures

Source: Author's own analysis

Figure 5.14 shows that 93% of participants agreed to a degree and to a full degree that adequate policies and procedures are necessary for effective continuity of operations during a crisis event. According to 7%, policies and procedures are important but to a lesser and more moderate degree. According to the literature, having detailed processes and procedures ensures the continued operation of business processes during times of crisis. The current applicability of this control measure is 95%. According to the information shown in Table 5.2, the mean of participants' views on the importance of developing adequate policies and procedures to ensure the continued operation of business processes during times of crisis is 4.93, which is higher than the mean of their views on current applicability, which is 4.29. In addition, the standard deviations for relevance and implementation status are 0.346 and 0.680, respectively. The degree of importance was lower than the degree of implementation, indicating that the data for the participants' views on importance were closer to the mean than the data for their views on applicability. The difference in means indicates that many participants agree that it is critical for organisations to have adequate policies and procedures in place to ensure that they can be effective in times of crisis, and it is suggested that this

practice is not fully recognised by all banks for applicability. However, the p-value = 0.000 level of significance demonstrates that there is substantial evidence that the means for importance and applicability of this control are noticeably different. According to the responses, having adequate processes and procedures as a risk control measure is highly regarded as important and applicable by most banks. As such, it can be deduced that banks should develop adequate policies and procedures to ensure the continued operation of business processes during times of crisis. The development of detailed processes and procedures can assist banks in achieving their risk management objectives and improving their preparedness for possible crisis events.

Question 15: Policies and procedures should stipulate effective communication strategies between all stakeholders to ensure the flow of essential business information, which should lead to continued business operations. Chapters 2 and 3 indicate the importance of adequate and continued communication during a crisis event. Figure 5.15 illustrates the responses.

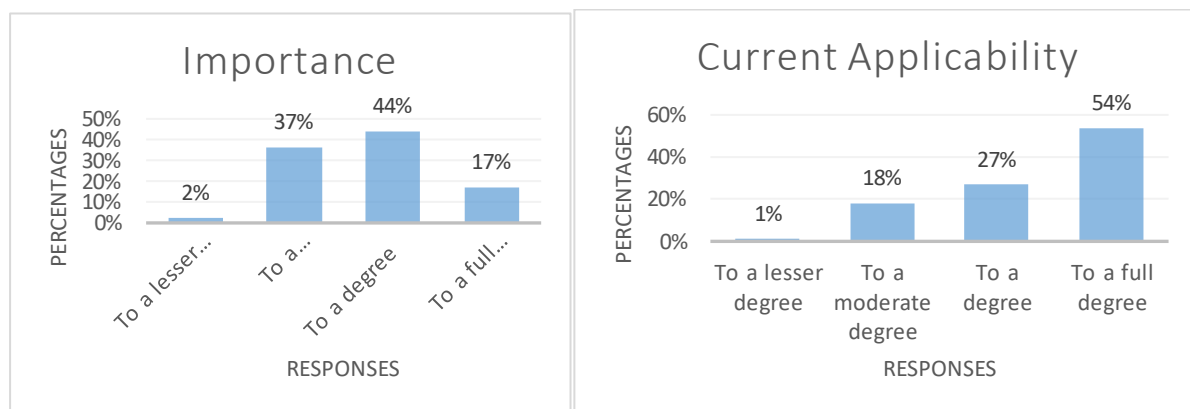


Figure 5.15: Communication strategies used during a crisis event

Source: Author's own analysis

Figure 5.15 shows that 61% of participants agreed that an organisation should develop policies and procedures that stipulate communication strategies that will be applicable during a crisis event. According to 39% of respondents, this risk control measure is important but to a lesser and moderate degree. The current applicability of this control measure is indicated by 81%, who agreed that there are adequate policies and procedures that stipulate how the bank will continue with communication during a crisis. However, 19% agree that this approach is applicable but to a moderate degree. The participants' mean opinion on importance is 4.90, which is higher than their mean opinion on current applicability, which is 3.76. This finding indicates that most respondents agree that policies and procedures must include effective communication strategies for all stakeholders to ensure the flow of critical business information and the continuation of business operations, and it also suggests that the current application

is not fully implemented. This is explained by the 1.14 gap in the current applicability based on the means of importance.

Furthermore, the data for participants' views on importance were closer to the mean than the data for participants' views on applicability were. This is explained by the fact that the standard deviation of importance is 0.300, which is less than the standard deviation of the current applicability, which is 0.767. The p-value in Table 5.2 equals 0.000, indicating that there is sufficient evidence that the mean importance of including communication strategies in policies and procedures and the mean of their applicability are not different. This confirms that participants regard the detailing of communication strategies used by the bank as an important operational risk control measure that provides a flow of essential business information to ensure continued business operations. Consequently, it seems that most banks have implemented this control measure.

According to the literature, communication strategies are an important aspect of business continuity throughout a crisis to help a bank achieve its goal of business continuity. For example, considering the recent global crisis, the COVID-19 pandemic, banks were forced to adapt to sudden changes such as switching to remote working and a massive shift to digital products. Therefore, it is critical that banks proactively identify alternative communication strategies to allow bank operations to continue during a crisis. Banks should ensure that all communication techniques are known to and accessible to all employees. As a result, appropriate training and awareness programmes seem essential for carrying out this risk control measure effectively.

Question 16: A business continuity management (BCM) policy should be approved and include a detailed business continuity planning (BCP) process that addresses a crisis. Figure 5.16 below shows participants' ratings of this question.

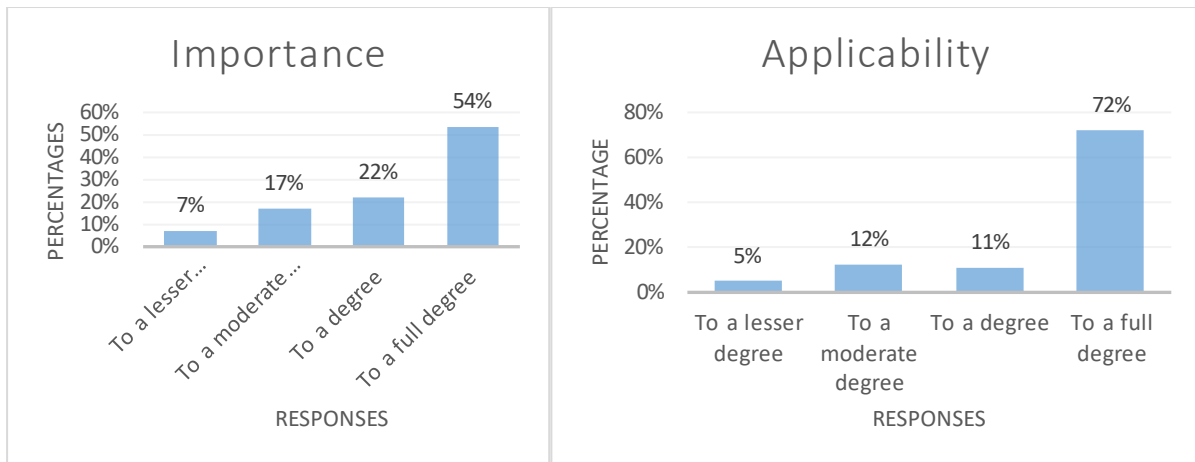


Figure 5.16: Business continuity management policy

Source: Author's own analysis

Based on the responses, 76% of the respondents agreed to a full degree that a bank should have an approved business continuity policy that includes a business continuity planning process that addresses a crisis. Twenty-four percent of respondents agree that this control measure is important but to a lesser and moderate degree. According to 83% of participants, this control measure is currently applicable, while 17% of participants rated it as applicable but to a lesser or moderate degree. A means comparison was also computed between the means of the participants about their views on the importance of approving a business continuity management policy and including a detailed business continuity planning process that addresses a crisis. The mean for views on importance is 4.78, which is higher than the mean for views on current applicability, which is 4.22. This is explained by the standard deviation of importance of 0.690, which is less than the standard deviation of the current applicability, which is 0.988 (refer to Table 5.2). A descriptive analysis identified a gap in the current applicability based on the means, with a variance of 0.56 from importance. This could indicate that while most banks see business continuity policies as crucial and apply them, some banks do not value this control measure. This may be because employees may be uninformed of the policy, which could result in a lower rating for implementation. However, statistical analysis indicates that there is significant evidence that the mean of participants' views on the importance of a bank having an approved BCM and the mean of their views on applicability are not different. Therefore, as indicated in the literature, banks need to develop and approve a business continuity management policy that includes a detailed business continuity plan on how to deal with a crisis. It is suggested that adopting the policy could ensure that a BCM policy includes all stakeholders who are responsible for maintaining the business's functioning during a crisis and that they are cognizant of their respective roles and responsibilities.

Question 17: A cybersecurity policy should include a process to ensure data and information security. This question suggests that a cybersecurity policy should include a process to ensure data and information security. Figure 5.17 below shows the results indicating the participants' ratings concerning this question and its present applicability.

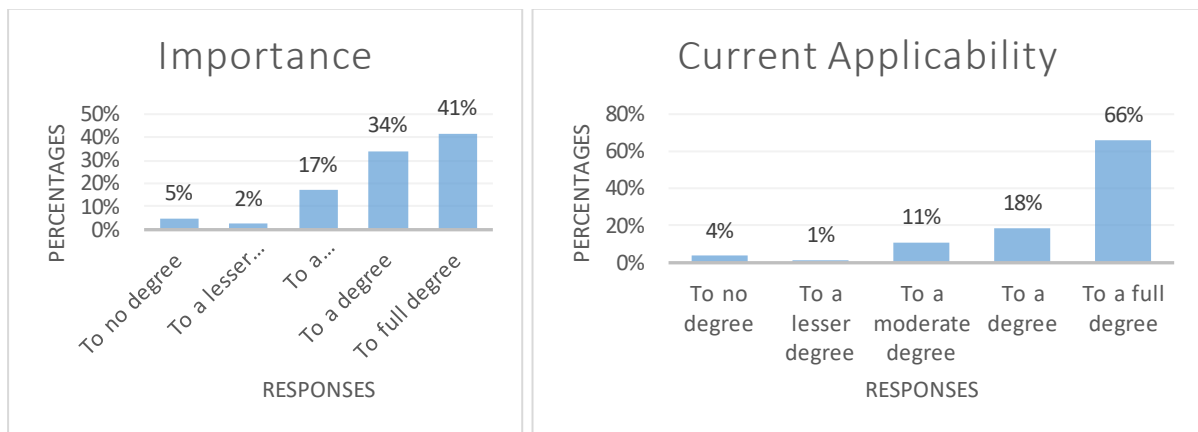


Figure 5.17: Cybersecurity policy

Source: Author's own analysis

Figure 5.17 shows that 75% of participants agreed to a degree or full degree that banks should develop cybersecurity policies that include a process to ensure data and information security. According to 19% of the respondents, banks have a cybersecurity policy but to a lesser or moderate degree, while 5% indicated that this control measure is unnecessary. The current applicability of this control measure is rated at 84%; however, 12% of respondents indicated that it is applicable but to a lesser or moderate degree, and 4% rated it as not fully implemented. The means of the respondents were compared in terms of the importance of developing and executing a cybersecurity policy that includes a process to ensure data and information protection. The importance and status of executing a cybersecurity policy that includes an organisation to ensure data and information security are 4.78 and 4.05, respectively. This indicates that the mean of importance is greater than the mean of the current applicability of this operational risk control measure, implying that most participants agree that it is important for a cyber-security policy to include a process to ensure data and information security, while the risk control measure remains unrecognised by some banks. This is explained by a gap in the current applicability, based on the means with a variance of 0.73 from importance.

Additionally, the standard deviation of importance is 0.759, which is lower than that for current applicability, indicating that the data on participants' views on the importance of ensuring that a cyber-security policy should include a process to ensure data and information security were closer to the mean than their views on applicability. According to the p-value of 0.001, the

mean importance and applicability of this control measure are not different. The literature has revealed that the increased use of technology and remote work due to the COVID-19 pandemic have exposed banks to several cyberattacks. This indicates that banks should be proactive in their cyber-security preparations. Therefore, the conclusion is that cyber security is crucial, although it seems that it is still not recognised by some banks, as explained by the means with a variance of 0.73. Banks should include a process to ensure data and information security in the cybersecurity policy of the bank to effectively achieve the goal of data protection and management.

Question: 18. A continuous training communication programme should be established to inform all stakeholders on cyber activities or threats. Figure 5.18 shows the respondents' ratings of the importance of continuing to train communication programme to inform stakeholders about cyber activities and threats. This further indicates whether banks currently apply the control measure.

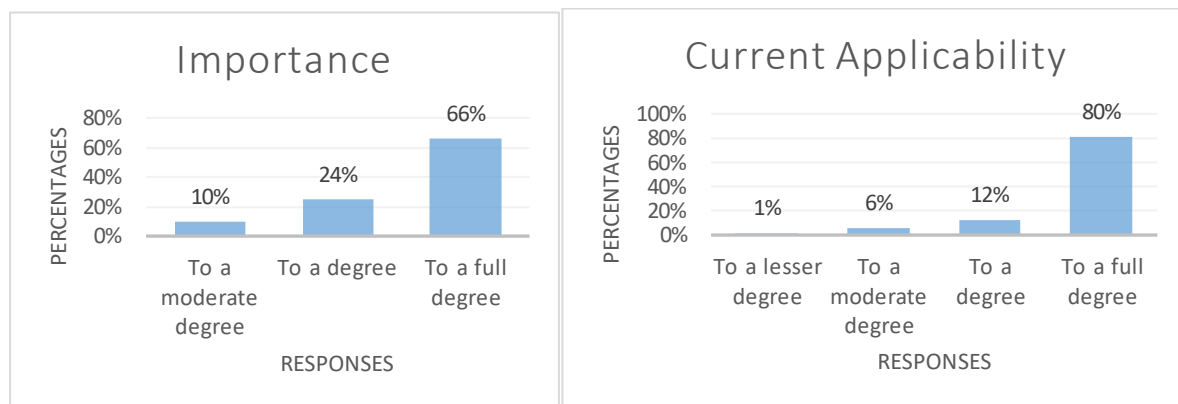


Figure 5.18: Communication programme

Source: Author's own analysis

As shown in Figure 5.18, 90% of the participants agreed or fully agreed that it is important to continually communicate cyber activities with all relevant stakeholders to increase cybercrime awareness (refer to sections 2 and 3 and sections 2.7 and 3.5, respectively). Ten percent of participants agreed, although to a moderate degree. This control measure is rated by most respondents and is currently applicable by most banks. This is confirmed by a rating of 92% for a degree and a full degree. However, 7% of participants agreed that banks have established training processes to inform all stakeholders of rising cyber threats and activities, although to a lesser or moderate degree. According to Table 5.2, most participants agree that it is critical to establish a continuous training communication process to inform all stakeholders on cyber activities or threats, and the current applicability is not directly proportional to importance, as indicated by the mean importance of 4.88, which is greater than the current

mean applicability of 4.56. Additionally, the data for participants' views on the importance of having a continuous training communication programme on cyber activities and threats were closer to the mean than their views on applicability. The 0.557 standard deviation of importance, which is less than the current applicability, which is 0.673, explains this. According to the p-value of 0.003, there is adequate evidence that the means for the importance and applicability of a continuous training communication programme for cyber activities and threats are not different. According to the literature, an increase in the use of technology by banks exposes banks to cybersecurity. Therefore, based on bank responses and examples of cyberattacks during the COVID-19 pandemic, cybersecurity training seems critical. Banks should establish communication channels to educate all stakeholders about cyber threats. Cybersecurity awareness should improve stakeholders' knowledge of cyber risk and their preparedness for cyber-attacks.

Question 19: A data backup facility should be established to protect an organisation from losing critical data due to a disruption caused by a crisis event. The respondents' ratings regarding the importance and current applicability of establishing a data backup facility to protect a bank from losing important data during a crisis event are shown in Figure 5.19 below.

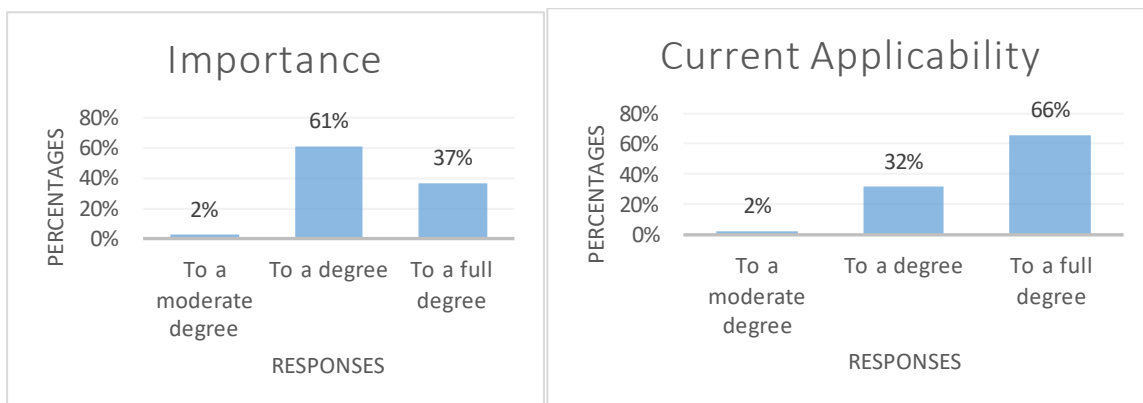


Figure 5.19: Data back-up facilities

Source: Author's own analysis

Figure 5.19 shows that 98% of participants rated to a degree or full degree that it is important for a bank to have a data backup facility. Figure 5.19 further shows that 98% of participants agreed to a degree and to a full degree that a bank should have a data backup facility to protect the bank from losing important data during a crisis event. The mean of the opinions on importance is 4.93, which is higher than the mean of the views on present applicability, which is 4.34. This implies that most participants agree that implementing this operational risk control technique to safeguard an organisation's data during a crisis is critical, although it is not equally implemented. This indicates a 0.59 variance in the means. The standard deviation of the

importance of this risk control measure is 0.346, which is higher than its applicability, which is 0.530. This indicates that participants' views on the importance of establishing data backup facilities were closer to the mean than their views on applicability. However, there is a statistically significant p-value of 0.000, which demonstrates that there is satisfactory evidence that the means for the importance of having a data backup facility and the means for its applicability are not different. The feedback indicates that banks understand the importance of developing a data backup facility as a risk control measure and have implemented it to ensure that the bank's data remain protected.

Question: 20. A BCM should be developed to ensure business continuity during a crisis. Figure 5.20 indicates the ratings on the importance of developing a BCM process to ensure business continuity during a crisis event and the current applicability thereof.

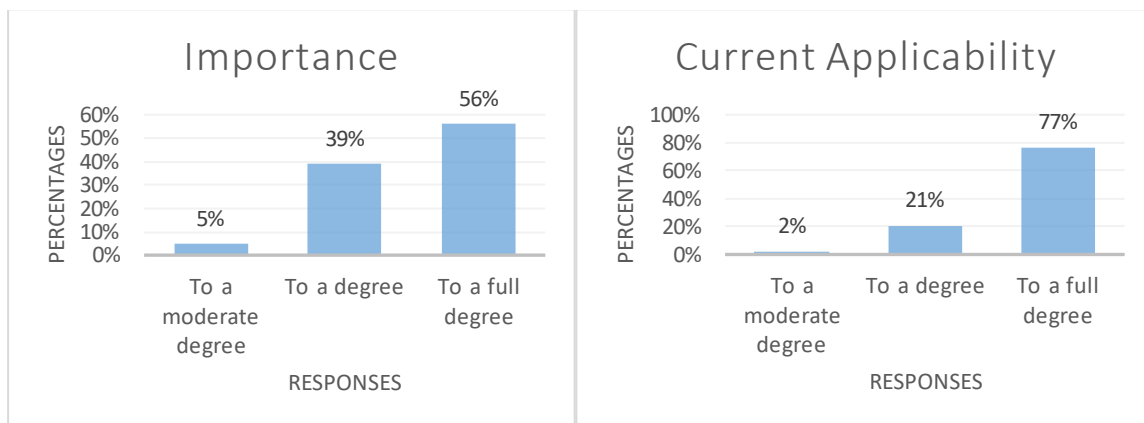


Figure 5.20: Business continuity management

Source: Author's own analysis

Figure 5.20 indicates that 95% of the respondents agree to a degree or full degree that banks need to develop a business continuity management process to ensure that a bank continues to operate during a crisis event. According to 5% of the participants, business continuity management is important but to a moderate degree. The current applicability of this control measure is 98%, while two percent of participants disagreed that this control measure is currently applicable, and 2% of participants indicated that it is unnecessary to have business continuity management.

A comparison of the means of participants' views on the importance of the BCM being established to maintain business continuity during a crisis and of its existing application indicated that the importance mean is 4.98, which is greater than the applicability mean of 4.51. This demonstrates that while most respondents believe that it is important for banks to develop BCM to ensure business continuity during a crisis, some banks are not prepared in

this regard. This is confirmed by the mean variation of 0.47 between the importance and the applicability of the BCM to ensure business continuity. The data on participants' views on the importance of a BCM were closer to its mean than their views on its applicability. However, the p-value of 0.000 indicates significant evidence that the mean importance of a BCM and the mean applicability are not different. Based on the responses, it can be deduced that banks understand and value the importance of business continuity management and its implementation as a risk control measure. As such, for effective management of operational risk during a crisis event, banks should have a documented business continuity management process that clearly explains how business will be conducted during a crisis. Therefore, business continuity management can be regarded as an important risk control measure for dealing with crisis events. In addition, it seems important that a bank convey a business continuity management process to employees to ensure that they understand the concept and their roles and responsibilities to ensure that the bank remains a growing concern and maintains operations during a crisis event.

Question 21: The BCM should indicate all stakeholders of the BCM. This question asked participants to rate the significance of indicating all internal and external stakeholders responsible for business continuity, as well as its current applicability as a control measure. Figure 5.21 presents feedback.

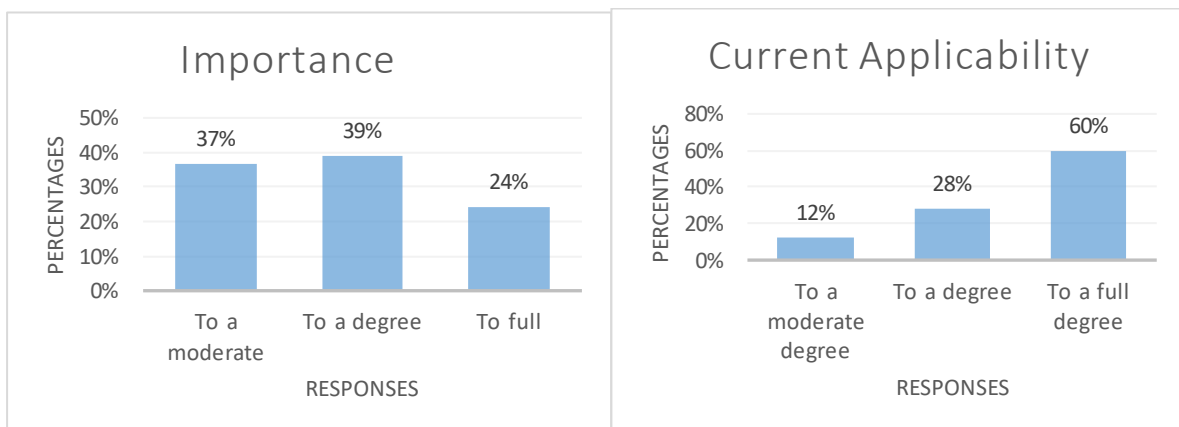


Figure 5.21: Inclusion of all stakeholders in the BCM

Source: Author's own analysis

Figure 5.21 shows that 63% of participants agreed that it is critical for a bank to include all stakeholders responsible for business continuity in the business continuity management process. In contrast, 37% of the participants agreed to a moderate degree. According to 88% of participants, this control measure is currently applicable, while 12% agree but to a moderate degree. The mean difference in participants' views on the importance of BCM indicating all stakeholders responsible for business continuity during a disruption was computed. The mean

opinion on importance is 4.83, which is higher than their mean opinion on existing applicability, which is 4.12. This shows that most respondents believe that it is critical for banks to indicate that all stakeholders are responsible for business continuity during a disruption in the BCM. It also suggests that this control measure has been adopted, although it indicates a variance of 0.71. Additionally, the results show that the standard deviation of the importance of including stakeholders in the BCM is 0.381, which is less than that for present applicability, which is 0.781. This indicates that participants' views on the importance of this control measure were closer to its mean than their views on its applicability. The study also looked for statistically significant evidence that BCM is important for indicating that all stakeholders are responsible for business continuity during a disruption. According to the results, the p-value is 0.000, which is less than 0.05, indicating that there is substantial evidence that the significance of this control measure and its applicability are not different. Most of the respondents agreed on the importance and applicability of this control measure for most of the banks. The literature has revealed that an effective BCM requires commitment from all levels of the organisation. Therefore, it is important that the BCM clearly indicate both external and internal stakeholders in BCM and their roles, for example, IT experts, external service providers, and senior management.

Question 22: BCM should include a process of dealing with a crisis that could disrupt the business or threaten the safety of employees. This question requires participants to indicate their rating regarding the importance and current applicability thereof. The responses are presented in Figure 5.22 below.

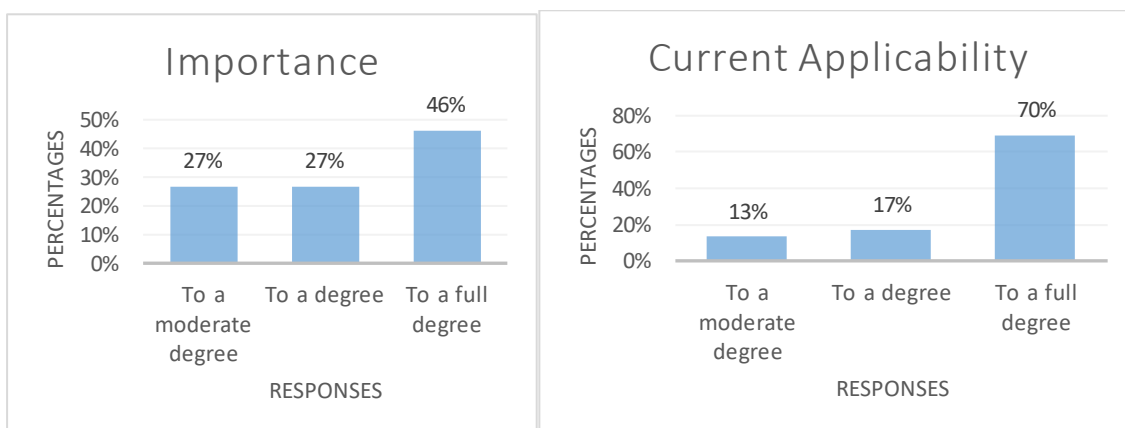


Figure 5.22: Crisis management

Source: Author's own analysis

Figure 5.22 indicates that 73% of participants agreed that BCM should involve the process of dealing with crisis events that could interrupt the business or endanger employees' health. However, 27% agree to a moderate degree. According to 87% of participants, banks have

implemented this control measure, although 13% agreed to a moderate degree. According to the literature, it is important that the process of managing a crisis event be indicated in the BCM. The 27% ambiguity may indicate that the importance of signalling the crisis management process is not well understood by other employees, resulting in 13% uncertainty regarding its implementation. As a result, it is critical to incorporate a process for dealing with crises that may disrupt the bank. Incorporating crisis management will guarantee that important personnel understand their individual duties and responsibilities in the event of a contingency. Furthermore, crisis management helps a bank establish a strategy for how it will respond to a crisis. A crisis management programme is an important instrument for proactive risk management to assist in determining which crises are most likely to affect the bank and what the business impact will be. As a result, the bank can plan proactive responses and adequately prepare its employees.

Question 23. A BCP should be defined to ensure that all stakeholders understand their roles and responsibilities during a crisis. This question required participants to indicate their opinion regarding the importance of defining a BCP to ensure that all stakeholders understood their roles and responsibilities during a crisis event. The responses are presented in Figure 5.23 below.

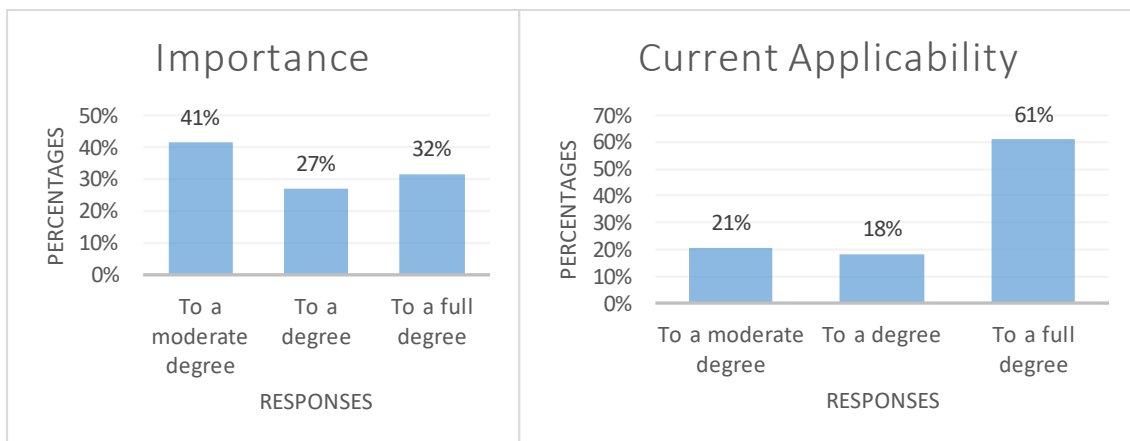


Figure 5.23: Business continuity plan (BCP)

Source: Author's own analysis

Figure 5.23 indicates that 59% of participants agreed to a degree and full degree that a bank should define a business continuity plan to ensure that all stakeholders understand their roles and responsibilities during a crisis, while to a moderate degree, 41% of respondents agreed that this control measure is important. The current applicability of this control measure is rated at 79%, while 21% of participants agree that it has been implemented, although to a moderate degree. However, the mean opinion on the importance of the BCP being established to ensure that all stakeholders understand their roles and responsibilities during a crisis is 4.90, which

is higher than their mean opinion on present applicability, which is 3.90. This implies that most participants agree that a BCP should be adequately defined and implemented. The data for participants' opinions on the importance of this control measure were closer to the mean than their views on present applicability. This is apparent because the standard deviation of importance is 0.300, which is less than the standard deviation of the current applicability. Therefore, there is statistically significant evidence that the participants' views on the importance of defining the business continuity plan and their views on its applicability are not different. This is confirmed by a p value of 0.000, which is less than 0.05.

The literature has revealed that it is important for banks to define their business continuity plan to ensure that stakeholders understand their responsibilities. Additionally, a BCP should clearly indicate recovery stages, critical functions, and employees responsible for critical functions. Additionally, to be better equipped to provide preventative mitigation against specific risk exposures, banks should develop a business continuity plan that clearly indicates potential scenarios of envisaged risk exposures. The business continuity plan should detail important aspects, such as alternative sites, that will be used during a crisis event. This approach can help banks better prepare for crisis events and function effectively when a crisis event occurs.

Question 24: Training drills should be performed to test the effectiveness of a BCP. Participants were prompted to share their thoughts on the significance of the banks in performing training drills to evaluate the effectiveness of the BCP and its implementation thereof. Figure 5.24 shows the results of the feedback.

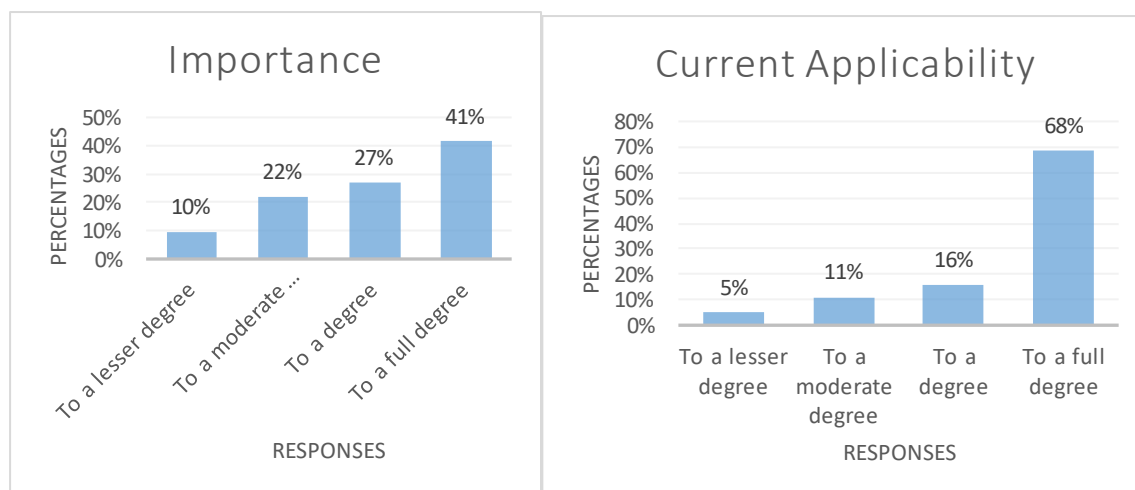


Figure 5.24 Training drills

Source: Author's own analysis

Figure 5.24 illustrates that 68% of participants agreed to a degree and to a full degree that training activities are necessary to verify the effectiveness of a BCP. According to 32% of participants, training drills are important but to a lesser or moderate degree. The current

applicability of this control measure is 84%, implying that training drills are currently available at the respective banks. However, 16% of participants indicated that it is applicable, although to a lesser or moderate degree. The differences in importance and applicability of 22% and 16%, respectively, could indicate that while banks have prepared business continuity plans, they have not been tested to guarantee that they will be effective during a crisis event. The mean opinion on the necessity of training drills to test the effectiveness of the BCP is 4.95, which is higher than the mean opinion on present applicability, which is 4.00. This finding implies that more participants agree that training drills are necessary to verify the effectiveness of the BCP and that the control measure is not equally adopted by all banks, as indicated by a mean variance of 0.95 between the importance and applicability of this risk control measure. This is explained by the standard deviation of importance of 0.218 being smaller than that for current applicability, 1.025. However, based on the p value of 0.000, as indicated in Table 5.2, there is sufficient evidence that the mean importance for training drills and the mean applicability of this control are not different. According to the literature, a business continuity plan should be assessed to confirm its effectiveness. Because crisis occurrences are unique, if a BCP is not consistently tested, it may become obsolete. As such, it is concluded that banks need to consistently perform drills to ensure the effectiveness of a BCP. Furthermore, an efficient business continuity plan mitigates the effects of business interruptions caused by a crisis event, potentially reducing the overall risk to the bank.

Question 25: A BCM should identify critical functions of an organisation that should remain operational during a crisis. Participants had to state their opinion regarding this operational risk control measure and its implementation status.

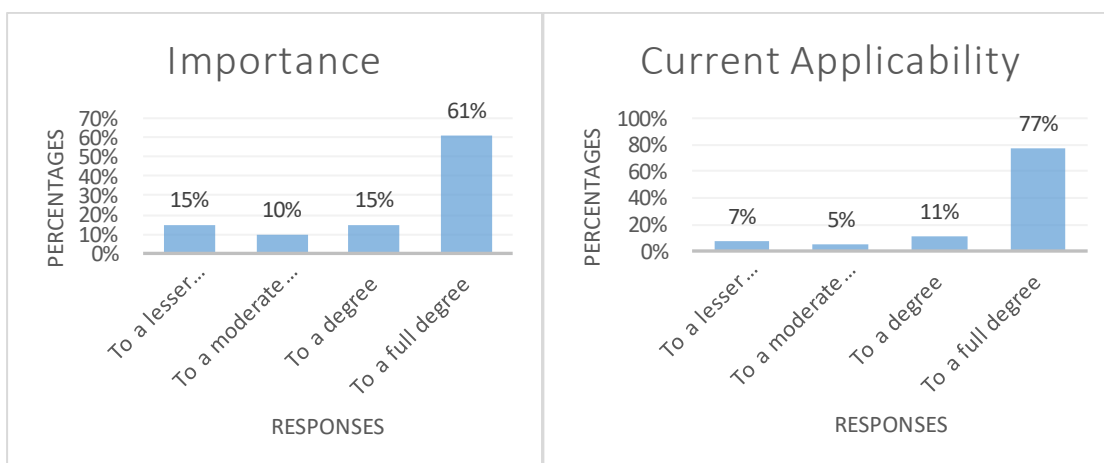


Figure 5.25: Identifying critical functions

Source: Author's own analysis

Figure 5.25 illustrates that 76% of participants agreed that it is essential to identify critical functions of the bank that must remain operational during times of crisis. According to 25% of the participants, critical functions are an important component of the business continuity management process; however, to a lesser or moderate degree. According to the feedback, most respondents regard identifying critical functions as an important risk control measure that will ensure banks' business continuity during a crisis event. The literature has confirmed that because of their essential nature, banks need to identify critical functions that must remain operational during a crisis. As such, 88% of the responses indicated that this control measure of identifying critical functions as part of the BCM process has been implemented by banks. However, 12% of the participants agreed that the intervention was implemented, although to a lesser or moderate degree. This could indicate that banks developed business continuity plans, but it seems that there is still room for improvement. The mean of their view on the importance of BCM for identifying critical functions of an organisation that should remain operational during a crisis is 4.93, which is greater than the mean of their view on the current applicability, which is 4.22. This suggests that most respondents concur that it is important for BCM to identify critical functions of an organisation that should remain operational during a crisis and further suggests that the current applicability is not directly proportional to importance. This is indicated by the variance of 0.76 in the mean importance of this control measure and its applicability.

The data for the participants' view on the importance of identifying critical employees were closer to the mean than their views on applicability. This is explained by the standard deviation of importance being 0.264 and being smaller than that for current applicability, which is 1.129. The p-value is 0.000, indicating that there is sufficient evidence that the mean importance and applicability of this control measure are not different. As such, the results show that participants regard identifying employees who will continue operating critical functions of the bank during a disruption as critical. It can therefore be concluded that it is crucial for banks to identify and prioritise their critical functions as a risk control measure during a crisis event, and these functions should form part of the banks' business continuity management. In addition, if important functions have been determined, suitable resources and responsibilities can be assigned during a BCP. Additionally, employee training is essential; therefore, determining critical functions will allow banks to ensure adequate training for employees responsible for executing the BCP. Therefore, critical functions are considered important components of an effective and proactive business continuity plan as a risk control measure that contributes to the effective management of banks' operational risk during a crisis.

Question 26: A BCP should stipulate which functions can be performed remotely during a crisis event. Figure 5.26 depicts participants' perspectives about the significance and state of implementation of indicating functions that can be performed remotely.

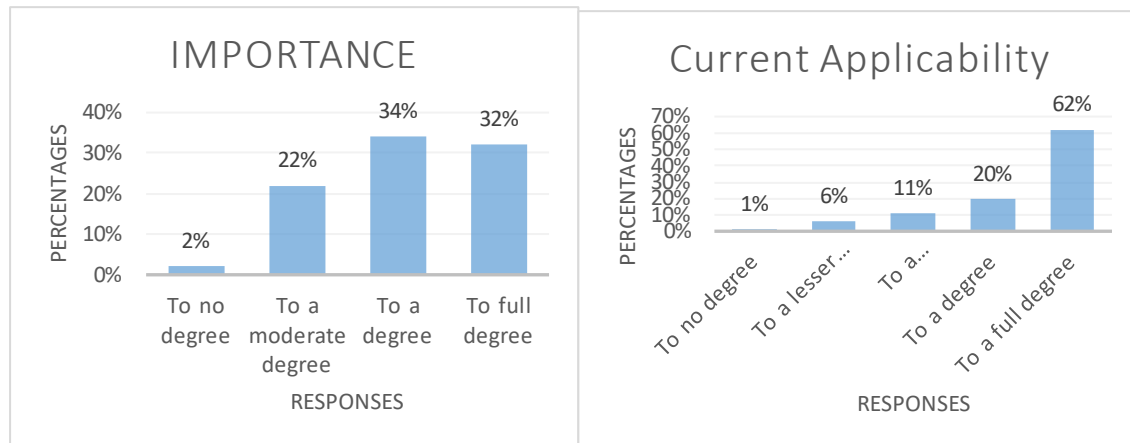


Figure 5.26: Remote working

Source: Author's own analysis

Figure 5.26 demonstrates that 66% of participants rated it critical that a BCP explain which functions can be performed remotely, while 32% of participants rated it to a lesser or moderate degree. Eighty-two percent of the responses indicate that the current BCPs have critical functions that can be performed remotely. However, there is uncertainty regarding the importance of this control measure and its applicability. It was confirmed that 32% of the responses had a lesser or moderate degree, and 2% of the responses indicated that this control measure was not significant. Additionally, 17% did not believe that the BCP indicates critical functions, while 1% disagreed that it is implemented. The comparison of means was computed between the means of respondents regarding their view on the importance of a BCP to stipulate which functions can be performed remotely during a crisis event. The mean of their view on importance is 4.88, which is greater than the mean of their view on current applicability, which is 3.83. This could indicate that although most respondents indicated that it is important for a bank to indicate in the BCP which functions can be performed remotely during a crisis event, the 1.05 variance in applicability based on the mean of importance could imply that the control measure has not been implemented in some banks. The data for the respondents' view on the importance of stipulating in the BCP which functions of the bank will be performed remotely during a crisis event were closer to the mean than their views on current applicability. This is explained by the standard deviation of importance being 0.510 and being smaller than the one for current applicability, 1.070. A p-value of 0.000 indicates that the mean importance of stipulating critical functions that will be performed remotely in the BCP and the mean applicability of this risk control measure are not different. According to the

literature, during the COVID-19 pandemic, tight restrictions were introduced to limit the spread of the disease; however, to comply with these restrictions, banks had to remain operational while reducing the number of employees working on site. As a result, certain functions must be performed remotely. As such, it is suggested that crisis events may necessitate performing additional responsibilities remotely, and banks should proactively identify these functions. This will allow employees to be adequately prepared prior to the commencement of a crisis event. In addition, banks can develop additional policies and guidelines and guarantee that employees have the necessary equipment and facilities to carry out operations remotely.

5.4. Concluding Remarks

This chapter presents the analysis of the survey as the empirical part of this study. The first section provided the participants' biographical information. The second section analysed the participants' views on the significance and implementation of the specified operational risk controls that could be used by a bank to prepare for a crisis in the form of descriptive statistics. Furthermore, inferential statistics were used to compare groups A and B and to substantiate relevant conclusions. According to the statistical analysis, all the identified risk control measures were confirmed to be critical for mitigating possible crisis events. Furthermore, all the controls are currently applicable to banks, although some require some attention to ensure their effectiveness.

The identified risk control measures are listed in Table 5.3 in order of priority, beginning with the risk control measure with the most significant mean rating.

Table 5.3: Priority of risk control measures

Priority of questions	Description	Importance mean rating	Applicability mean rating	Variance
7	Risk identification	4.98	51	0.47
20	Business continuity management	4.98	4.51	0.47
24	Training drills	4.95	4.00	0.95
10	Risk monitoring	4.95	4.05	0.90
1	Definition of operational risk	4.93	3.66	1.27
13	Health and safety environment	4.93	4.02	0.91
22	Crisis management	4.93	4.20	0.73
25	Identifying critical functions	4.93	4.22	0.71
14	Policies and procedures	4.93	4.29	0.64
19	Data back-up facilities	4.93	4.34	0.59
15	Communication strategies to be used during a crisis event	4.90	3.76	1.14
12	Training of employees	4.90	3.88	1.02
23	Business continuity plan	4.90	3.90	1.00
9	Risk control and mitigation	4.90	4.37	0.53
26	Remote working	4.88	3.83	1.05
8	Risk evaluation	4.88	4.37	0.51
18	Communication process	4.88	4.56	0.32
3	Risk culture	4.83	3.59	1.24
21	Including all stakeholders in BCM	4.83	4.12	0.71
11	Appointing employees for critical functions	4.8	4.24	0.56
5	Governance structure	4.8	4.37	0.43
4	Risk management strategy	4.78	3.98	0.80
17	Cyber- Security	4.78	4.05	0.73
16	Business continuity management policy	4.78	4.22	0.56
2	Operational risk management framework	4.71	3.80	0.91

Source: Author's own analysis

Although all the risk control measures were identified as important for effectively preparing and managing crisis events, only the first five are highlighted.

The highest priority can be identified as the inclusion of risk identification as a step of an operational risk management process to identify inherent risk exposures. This is explained by the highest mean importance rating of 4.98. As indicated in the data analysis, 98% of participants agreed to a degree and to a full degree that risk identification must be a component of the risk management process of a bank to assist the bank in achieving the objective of effective risk management. As such, it appears to be the most important risk control measure that banks should implement to proactively prepare for a crisis. Therefore, to effectively prepare for a crisis event, banks should include risk identification in their risk management process. This approach will assist employees in identifying and understanding the inherent risks that banks could be exposed to.

The second priority risk control measure is the development of a business continuity management (BCM)

process. This is explained by the mean importance rating of 4.98. The findings indicated that 95% of participants agreed that it is important for a bank to develop a business continuity management process to ensure that it continues to operate during a crisis. As such, banks need to have a documented business continuity management process that clearly explains how business will be conducted during a crisis. Banks should also ensure that they convey the business continuity management process to all employees to ensure that they understand the concept and their roles and responsibilities to ensure that the bank continues with its business operations during a crisis event.

The third important risk control measure for banks to implement and prepare for a crisis is training drills. This entails the banks performing training drills to test the effectiveness of the business continuity plan. This is explained by the mean importance of 4.95, where 68% of participants agreed to a degree and full degree that the risk control measure is important, and 32% more participants agreed to the importance of this risk control measure, although to a moderate degree. As such, banks should constantly test their BCPs to ensure that they remain effective despite the occurrence of a changing crisis. The BCP may need to be updated to suit a specific crisis event because as a crisis occurs, a different approach may be needed. This approach will ensure that the BCP remains effective at sustaining any crisis event.

The fourth important risk control measure is risk monitoring, which entails continuous monitoring of risk controls to ensure that they remain effective. This is confirmed by the mean importance rating of 4.95, with 73% of participants agreeing to a degree and to the full degree that this control measure is important and 27% of participants agreeing but to a moderate degree. It is important that banks monitor risk control measures and address risk monitoring in policy documents to specify the roles and responsibilities of the role players. This exercise will ensure that banks proactively detect gaps in risk controls and rectify them accordingly.

The fifth most important risk control factor is defining operational risk, with a mean importance of 4.93; 63% of participants viewed this risk control measure as important. Defining operational risk will ensure that all employees of the bank understand it to enable us to identify operational risk exposures that banks could be exposed to. As such, banks ought to define operational risk adequately to ensure that it is understood by all employees and to enable them to identify specific operational risks that banks could be exposed to due to a crisis event. This exercise will allow banks to proactively manage the identified risk exposures. However, all the risk control measures identified by this study are deemed important for banks to adopt to prepare for crisis events.

Table 5.4 depicts the top ten risk controls with the greatest mean variance between importance and applicability of the risk control measures, which could indicate that

attention is required to enhance the applicability of risk control measures to align them with the rated importance.

Table 5.4: Top 10 risk control measures with the highest variance between importance and current applicability

Priority of Questions	Description	Importance Mean Rating	Applicability Mean Rating	Variance
1	Definition of operational risk	4.93	3.66	1.27
3	Risk culture	4.83	3.59	1.24
15	Communication strategies to be used during a crisis event	4.9	3.76	1.14
26	Remote working	4.88	3.83	1.05
12	Training of employees	4.9	3.88	1.02
23	Business continuity plan	4.9	3.9	1.00
24	Training drills	4.95	4	0.95
13	Health and safety environment	4.93	4.02	0.91
2	Operational risk management framework	4.71	3.8	0.91
10	Risk monitoring	4.95	4.05	0.90

Source: Author's own analysis

While all the control measures were rated as important and applicable, only the top five questions according to the priority list will be discussed in more detail.

The first risk control measure, with a greater difference between its substance and existing applicability, is to adequately define operational risk in banks to assist employees in recognising potential risks to which banks may be exposed. The 1.27 variance could indicate that there is a gap in the application of this control measure. As a result, it is suggested that banks improve their communication within the bank to confirm the definition of operational risk and to describe operational risk components such as processes, people, systems, and external risk factors. This control measure is also listed under the top five of the priority list, confirming its importance. Therefore, it can be concluded that this control measure is crucial, and banks should ensure that a definition of operational risk is included in risk policies and that all stakeholders are aware of its meaning and their roles and responsibilities regarding risk management.

Question 3, which concerns risk culture, is the second risk control measure that indicates a greater variance between the mean of importance and its applicability. This is indicated by a variation of 1.24 between the mean of importance of a bank ensuring the embedding of norms, attitudes and behaviours of employees relating to risk controls. This variation could imply that although respondents view risk culture as an important risk control measure that banks should adopt to achieve the objective of effective risk management, it has not been implemented adequately by some banks. As such, leadership is critical in setting the tone for successful application of a strong risk management culture, while risk knowledge, communication, risk appetite, employee participation, learning from mistakes, and proactive adaptation to the regulatory environment are all important components of a strong risk culture. By emphasising risk culture, banks may successfully manage risks, develop resilience, overcome uncertainties, identify emerging risks, and make informed decisions.

The third important risk control measure that seems to have not been implemented in some banks is ensuring that the policies and procedures of the banks stipulate effective communication strategies between all stakeholders to ensure the flow of business information, which should lead to a bank's business continuity during a crisis. The 1.14 variation based on the means of importance of this risk control measure could indicate that communication strategies are not clearly stated. This could also mean that the strategies are known by top management only instead of by all stakeholders. As such, it is important for banks to ensure that this control measure of communication strategies is clearly stated and documented in the policies and procedures of the bank to ensure that it is known and accessible to all employees. This can be achieved through adequate training and awareness programmes. Additionally, it is recommended that banks establish a crisis communication plan and perform postcrisis evaluation and follow-up communication. This should assist banks in improving and specifying strategies for communication during a crisis.

Question 26 entails the importance of identifying and indicating which functions of the bank can be operated remotely during a crisis event and is the fourth risk control measure, with a greater variance in applicability of 1.05. This variation could imply that although this control measure has been implemented, some banks are still lacking in terms of which critical functions can be operated remotely. Additionally, although the functions have been identified, banks might not have appropriate resources to carry out those operational functions remotely. Therefore, it is recommended that banks identify critical functions that can be operated remotely during a crisis, ensure the acquisition of appropriate infrastructure and assign appropriate resources that will enable the implementation of this control measure. Furthermore, banks can develop additional policies and guidelines and guarantee that employees have the necessary equipment and facilities to carry out operations remotely.

The fifth risk control variable, which has the highest variance between importance and applicability, is the training of employees to ensure that they understand and can perform their functions during a crisis event. The 1.02 variation could indicate that employees were not adequately informed about their responsibilities during a crisis. As such, it is suggested that banks provide essential skills and knowledge to their employees to ensure that they can effectively conduct their operations during a crisis. Therefore, it is important that banks perform drills to ensure that employees understand their roles and responsibilities during a crisis.

Although the identified and analysed risk control measures are non-exhaustive, the findings suggest that the identified measures are critical for a bank to implement to prepare for a crisis event. The most significant conclusions are summarised in the next chapter, which will serve as the basis for this study's recommendations.

CHAPTER 6: SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

6.1. Introduction

The preceding chapter addresses the statistical examination of the survey data and the relevant findings in terms of the identified risk control measures to prepare for and address a crisis event. These findings will help recommend the importance and application of operational risk control measures. This chapter will begin with a description and outline of the intentions of the study and then conclusions and suggestions on how banks should assure the applicability of important risk control measures to enhance their preparedness for a possible crisis event. Furthermore, it will highlight the study's influence on the amount of information, its shortcomings, and suggestions for additional future studies.

6.2. Summary of the Study

The prior five chapters of the study are summarised below:

Chapter 1: This chapter presents background information and a summary of the available literature, emphasising the current state of the banking industry in Lesotho as well as the key risks that banks face. The problem statement, research objectives, and research questions were established, and a brief description of the research methodology, as well as ethical considerations and study limitations, was provided.

Chapter 2: This chapter offers an overview of the relevant risk management literature. The objective of this research is to identify operational risk control measures that will assist banks in preparing for and protecting themselves from potential operational risk exposures during crisis events. To achieve these goals, the researcher reviewed risk management frameworks to identify common framework components. Furthermore, the chapter identifies and assesses operational risk to confirm operational risk factors. An evaluation of the identified operational risk factors was performed to identify potential risk control strategies.

Chapter 3: This chapter discusses the COVID-19 pandemic and the underlying operational risk exposures associated with the indicated risk controls identified in the literature.

Chapter 4: This chapter describes the research design utilised for this study, providing additional details on the research methods used to collect the data and the numerical methods used to analyse the data.

Chapter 5: Based on a statistical and descriptive analysis of the questionnaire responses, this chapter analyses and interprets the survey findings about the importance of operational risk control methods and their current applicability in various banks.

6.3. The Purpose and objectives of the Research

- The purpose of this study was to determine operational risk control measures to prepare and safeguard banks from potential operational risk exposures during crisis events based on the experiences of the COVID-19 pandemic. To support this purpose, the primary objective of the study was to identify the effect of the COVID-19 pandemic on the operational risk faced by the Lesotho banking industry and to determine preventative control measures
- The following secondary objectives were identified:
- To conduct a literature review on operational risk to serve as a platform to identify control measures for a bank during a crisis event.
- To review the main influences of the COVID-19 pandemic on operational risk and the underlying risk factors faced by banks in Lesotho to confirm appropriate control measures to protect banks from similar future events.
- To perform an empirical analysis of the identified risk control measures for operational risk by using descriptive statistical analysis to determine their importance and applicability. The findings of the analysis of the identified control measures to protect and prepare banks against crisis events were used to verify the contemporary applicability of the identified controls and serve as a platform for recommendations to realise the intention of the research.

The next section details the findings of the study in accordance with the objectives.

6.4. The Results of the Survey

The results of the survey are explained in the following sections.

6.4.1. Operational risk control measures

The literature review was used to identify operational risk control measures that are appropriate for preparing for a crisis event. Further literature reviews of the COVID-19 pandemic were conducted to identify operational risk exposures for each underlying risk factor. Following the literature review (refer to sections 2.7 and 3.5), 26 operational risk control measures were identified (Table 5.3). Table 5.3 displays the identified risk control measures and descriptions in descending order of importance, beginning with the control measure with the most important rating and progressing to the one with the least amount of importance.

Table 5.3: Identified operational risk controls and their description

Priority of questions	Risk control	Description
-----------------------	--------------	-------------

7	Risk identification	This control measure entail including risk identification as a step of risk management process ensure that banks proactively identify and mitigate the inherent risks that the crisis occurrence may expose them to.
20	Business continuity management	This entails a development of a BCM to ensure business continuity during a crisis event.
24	Training drills	Entails performing training drills to test the effectiveness of a BCP.
10	Risk monitoring	Entails continuous monitoring of the risk controls to ensure that they remain effective, even with the changing environment or crisis situations.
1	Definition of operational risk	Entails a clear definition of operational risk, to ensure that all employees understand what operational risk is, so that they able to identify operational risk factors that banks may be exposed to.
13	Health and safety environment	This risk control measure is concerned with provision of a health safety environment for employees during a crisis event.
22	Crisis management	This risk control measure demonstrates the need for banks to ensure that they develop a crisis management plan, which must be included in the BCM. The plan will indicate the steps for dealing with a crisis or a disruptive situation.
25	Identifying critical functions	This entails identifying critical functions of the bank that must remain operational during a crisis. This will all adequate allocation of relevant resources.
14	Policies and procedures	developing adequate policies and procedures, that will ensure the continued operations of business processes during times of a crisis.
19	Data back-up facilities	Establishing a data backup facility to protect an organisation from losing critical data due to a disruption caused by a crisis event.
15	Communication strategies to be used during a crisis event	Policies and procedures should stipulate effective communication strategies between all stakeholders to ensure the flow of essential business information, which should lead to continued business operations.

12	Training of employees	Provision of training of critical employees, to ensure sure that they have the skills and knowledge to perform critical functions.
23	Business continuity plan	Developing a business continuity plan and ensuring that it clearly defined to be understood by all employees of the bank.
9	Risk control and mitigation	Incorporation risk control and mitigation as a step of an operational risk management process. This will assist the bank to establish risk control measures for the identified risks.
26	Remote working	A BCP should stipulate which functions can be performed remotely during a crisis event.
8	Risk evaluation	Risk evaluation should be a step of an operational risk management process to assess the identified risks in terms of likelihood and impact.
18	Communication process	Establishing a continuous training communication programme to inform all stakeholders on cyber activities or threats.
3	Risk culture	This entails instilling a risk management culture within the bank. A risk culture should embed norms, attitudes and behaviours of employees relating to risk controls.
21	Including all stakeholders in BCM	This control entail indication of all internal and external stakeholders who will be needed to continue business during a crisis in the BCM. For example, IT support and suppliers.
11	Appointing employees for critical functions	This risk control measure entails identifying critical employees who will perform critical functions of thee bank during a crisis. This will assist the bank to provide adequate training to such employees and ensure that they understand their roles and responsibilities during a crisis.
5	Governance structure	This entails the embedding of governance structure to confirm roles and responsibilities of the role players of risk management.

4	Risk management strategy	Entails aligning risk management with the business strategy to guarantee that the objectives are within the set limits of the risk appetite.
17	Cyber- Security	It entails having a process that ensures data and information security and the process must be included in the BCM.
16	Business continuity management policy	A BCM policy should be approved and include a detailed Business Continuity Planning (BCP) process that deals with a crisis.
2	Operational risk management framework	An operational risk management framework should be embedded to serve as a platform to guide effective operational risk management.

Source: Author's own analysis

6.4.2. Confirmation of the identified risk control measures

The identified risk control measures were assessed through a questionnaire-based survey, which determined respondents' perspectives on the importance and applicability of such measures within their respective banks. Based on the findings, it was concluded that all identified risk control measures should be implemented by a bank to prepare for a crisis event. It was also stated that all the identified risk control measures had been adopted by banks to some degree.

6.4.3. Data analysis

The empirical study of the data supported the significance and application of the identified risk control measures. The variation in research between the importance and current applicability ratings allowed for findings and recommendations to be made to affirm the importance and applicability of the identified risk mitigation strategies. According to the findings, most respondents agreed that the risk-control measures listed were important. However, it was clear that there is a gap, which could imply that, while banks have developed risk control procedures, not all are applied to an acceptable level. As a result, recommendations were issued to assist banks in enhancing the implementation of these risk control measures.

6.5. Study Constraints

Although this research was as comprehensive as possible, it has several limitations. The first constraint is that it was limited to individuals who were engaged in operational risk management in the Lesotho banks. The scope of the study excludes all other risks such as credit risk, reputational risk, and market risk. The next constraint was data accessibility owing to the sensitivity of the organisation's information. The study expected five banks to participate

in the survey, but only three accepted the survey due to the sensitivity of data. However, the information gathered was deemed adequate to support the study's findings. The recommendations are summarised in the next section.

6.6. Recommendations

This section offers a summary of the study's conclusions according to the empirical analysis. The conclusions are based on the significance and applicability of the identified risk control measures. According to the statistical analysis, all the operational risk control measures were confirmed to be important and applicable for banks to prepare for crisis events. According to the survey, all of the identified risk control measures have been implemented by the participating banks to some degree. The conclusions of the descriptive analysis of the identified control measures culminated in recommendations on how banks might improve on these risk controls to assure their sustained efficacy. A summary of these recommendations is as follows:

- **Risk identification:** The objective was to emphasise the significance of a bank incorporating risk identification as a step in the risk management process. Risk identification must be included in the risk management process for banks to achieve the objective of effective operational risk control during a crisis. As a result, it is recommended that this is an important risk control measure that banks should employ to fulfil their business objectives and ensure that banks proactively identify and mitigate the inherent risks that the crisis may expose them to.
- **Business continuity management:** The objective was to demonstrate the importance of banks adopting a business continuity process to ensure the continuation of business operations during a crisis. The study concluded that the BCM is a critical operational risk control method that banks should employ to assure their preparedness for a crisis event. As such, banks should design a business continuity management process and guarantee that all workers understand the concept and clearly define workers' roles and responsibilities during a crisis.
- **Training drills:** This emphasises the importance of a bank conducting training drills to assess the effectiveness of a business continuity plan (BCP). Since each crisis is unique in terms of causes and consequences, banks should conduct drills on a regular basis to ensure that the BCP remains effective at addressing all aspects of a potential crisis event.
- **Risk monitoring:** A risk monitoring step must be incorporated into the process of risk management to continuously monitor risk controls for efficacy. It is recommended that the risk monitoring process be addressed in the policy documents of banks to define the roles and responsibilities of all role-players regarding the continuous analysis and

updating of risk control measures. This could allow banks to proactively recognise and rectify weaknesses in risk control measures.

- **A comprehensive explanation of operational risk:** Banks need to embed a clear definition of operational risk to contribute to effective risk management. This approach could ensure that all employees understand the concept and what is required to embed effective operational risk control measures to proactively prepare for potential crisis events.
- **Health and safety environment:** The objective of using a healthy and safe environment as a risk control measure was to confirm the importance of providing a safe and healthy environment for employees during times of crisis. Banking was determined to be an essential service that must remain operational during a crisis. As a result, bank employees are exposed to potential health risks because they are obliged to work during a crisis. Thus, it is recommended that banks provide all the necessary resources to employees, depending on the event, to ensure their health and safety. Furthermore, safety drills and procedures for how employees should protect themselves during a crisis event are some of the steps that a bank should provide to its employees to ensure the objective of effective proactiveness and crisis preparedness.
- **Crisis management:** This underlines the need to include a method for responding to a crisis that could disrupt a business or threaten employees. It was established that embedding a business continuity management process is a crucial risk control measure for banks. This approach could ensure that key employees understand their distinctive duties and obligations in the case of a crisis. Furthermore, banks should develop a crisis management strategy that can anticipate which crises are most likely to affect them and what their business impact will be. As such, appropriate proactive responses can be identified.
- **Identifying critical functions:** It has been determined that identifying critical functions is an important risk control measure that banks should consider preparing for crisis events effectively and proactively. The identified critical functions should be included in a bank's business continuity management process. It seems that if critical functions have been identified, appropriate resources and responsibilities can be assigned during a BCP. Furthermore, it is recommended that adequate training be provided to employees who are responsible for executing the BCP.
- **Policies and procedures:** This control measure entails developing and implementing adequate policies and procedures to ensure that businesses can continue to operate during times of crisis. In this regard, banks should develop thorough processes and

guidelines to assist them in achieving their risk management objectives and strengthening their preparedness for potential crises.

- **Data backup facilities:** This risk control measure entails establishing a data backup system to safeguard banks from losing critical information. It was concluded that this risk control measure is critical, and it is recommended that banks develop data backup systems to assure data security and protection before and during crises.
- **Communication strategies:** Banks should develop communication strategies that should be included in their policies and processes to ensure the proper flow of critical business information that leads to adequate business continuity. It is recommended that banks ensure that all communication strategies are known and available to all employees. This could be achieved by implementing proper training and awareness campaigns. Furthermore, banks should develop a crisis communication plan and conduct postcrisis evaluation and follow-up communication to assist in improving communication tactics during a crisis.
- **Training of employees:** This risk control measure entails employees who are trained to ensure that they understand and can perform their duties during a crisis. This control measure has been determined to be critical for ensuring that all employees understand their role and responsibilities during a crisis event. In this regard, it is recommended that banks conduct training and emergency drills on a regular basis to ensure that employees understand their duties and responsibilities during a crisis. Furthermore, banks should provide the necessary skills and knowledge to employees to guarantee their activities during a crisis.
- **Business continuity plan:** This risk control measure comprises developing a business continuity plan (BCP) to ensure that all stakeholders understand their roles and responsibilities during a crisis. It was concluded that banks need to develop a business continuity plan that clearly outlines potential scenarios of anticipated risk exposures. The business continuity plan should include critical details such as alternate sites that will be used in the event of a crisis. This approach can help banks prepare more effectively for crisis events.
- **Risk control and mitigation:** It is concluded that BCM is an outcome of operational risk control against a crisis. Therefore, it is critical that the BCM be implemented in a bank's risk management process as an operational risk control tool, which could contribute to effective crisis management. This can be achieved by providing every employee with risk control and mitigation training to prepare for risk exposure and potential crisis events.

- **Remote working:** During a crisis event, banks may decide to perform additional activities remotely. As such, it is suggested that banks identify critical operations that can be operated remotely in the event of a crisis and ensure that necessary infrastructure and resources are acquired and assigned to enable the adoption of this control measure. Furthermore, banks should adopt additional guidelines and procedures and ensure that employees have the appropriate technology and facilities to conduct operations remotely.
- **Risk evaluation:** Risk evaluation was confirmed to be an important step in the operational risk management process that involves evaluating identified risks in terms of possibility and impact. Therefore, risk evaluation should be included in the risk management process to ensure a bank's objective of effective operational risk management and to prepare for potential crisis events, as it can also be viewed as providing a platform for the formulation of risk control and mitigation measures.
- **Communication processes:** Cybersecurity appears to be an important control measure for protecting banks from cyber threats. As a result, banks need to establish communication channels to educate all stakeholders about cyber risks. Cybersecurity awareness should increase stakeholders' understanding of cyber risk as well as banks' and stakeholders' preparedness for cyberattacks. Training is a crucial tool for ensuring that this control measure is implemented effectively.
- **Risk culture:** The embedding of a risk culture was found to be an important operational risk control measure. Thus, it is suggested that banks employ a risk culture that embeds the norms, attitudes, and behaviours that will lead them towards effective risk management. Additionally, it was found that leadership is critical for this control measure. Leaders should set the tone for successful implementation of a strong risk management culture. Furthermore, risk knowledge, communication, risk appetite, employee participation, learning from mistakes, and proactive adaptation to the regulatory environment are all important factors of a strong risk culture. It is envisaged that by embedding a risk culture, banks may successfully manage risks, develop resilience, overcome uncertainties, identify emerging risks, and make informed decisions.
- **Including all stakeholders in BCM:** It appears that numerous stakeholders, for example, external service providers, technology specialists, and senior management, contribute to a bank's business continuity. As such, it was concluded that it is critical that a bank's BCM process involve all stakeholders. As such, banks should establish a BCM process that clearly identifies both external and internal stakeholders and their responsibilities.

- **Appointing employees for critical functions:** During a crisis, it is necessary for a bank to appoint employees who will be responsible for specified critical functions. It is essential that banks ensure that they have adequate personnel to support them through a crisis. Furthermore, critical employees must be provided with the necessary resources to enable them to continue their business during a crisis. Training is an important instrument that banks can use to effectively apply this control measure.
- **Governance structure:** Banks should ensure the establishment of a governance structure to confirm the responsibilities and obligations of all role-players in risk management. Therefore, it is recommended that governance structures be updated to address a changing environment, particularly considering recent global events such as the COVID-19 pandemic, to ensure that a bank is prepared for such events and that all role-players are aware of their respective tasks and responsibilities.
- **Risk management strategy:** This risk control approach involves aligning a bank's risk management strategy with its business strategy to guarantee that objectives remain within risk appetite limits. As such, banks should clearly state their limits, targets, and thresholds for various operational risks. This will guarantee that the objective of the bank's risk management strategies remains within the operational risk limits. Furthermore, a bank should ensure that all employees are aware and understand the resulting risk appetite, which is a critical operational guideline, including being prepared for future crisis events.
- **Cybersecurity policy:** Banks should develop a cybersecurity policy that includes a process for ensuring data and information security. To effectively achieve the goal of data protection and management, banks should include a process to ensure data and information security in their cybersecurity policy.
- **Business continuity management policy:** A bank should have a BCM policy that has been approved and includes a defined business continuity process for dealing with a crisis. It is recommended that banks employ this risk management measure to ensure that a BCM policy involves all stakeholders who are responsible for business continuity during a crisis and are cognisant of their roles and responsibilities.
- **Operational risk management framework:** This risk management measure comprises incorporating an operational risk management framework as a platform to guide effective operational risk management. The incorporation of an operational risk management framework has been confirmed to be an important risk control measure. Therefore, an operational risk management framework should be implemented to serve as a platform for effective operational risk management within a bank.

6.7. Research Contribution

This study can add to the knowledge base of operational risk management and endeavours to improve the understanding of operational risk control measures applicable to preparing for potential crisis events. Although the study involved the experience and views of banks, the identified non-exhaustive list of risk control measures can be applied by all organisations to identify and prepare for potential crisis events. Banks may apply these operational risk controls and mitigations, increasing their preparedness for crisis events. Furthermore, the identified risk controls can be used as a checklist (see Annexure H) for businesses to review their status and progress in implementing operational risk controls to prepare and safeguard banks from a crisis event.

6.8. Suggestions for Additional Research

The research intended to determine risk control measures that the Lesotho banking industry could employ to prepare for crisis events, similar to what was experienced by the COVID-19 pandemic. The investigation showed that every identified risk control is important and has been implemented by banks to a certain degree. However, the identified risk controls mostly revolve around the preparedness of a potential crisis event and do not necessarily include risk control measures during normal business operations. As such, further study could focus on risk control measures applicable for specific business operations, such as during a supply chain management process. Furthermore, this study focused only on operational risk; therefore, a future study could include risk control measures for additional risk types, including reputational risk, credit risk and market risk.

6.9. Chapter Conclusion

This investigation determined and validated operational risk control measures that the Lesotho banking industry can adopt to prepare for potential crisis events. An empirical investigation was carried out to verify the importance of the identified risk control measures and their applicability. The significance of the identified risk control measures became apparent throughout the study. However, although all risk control measures were confirmed to be critical, the research also confirmed gaps in the current applicability thereof. Therefore, the results of this study can be used by banks to evaluate their existing position and address issues while creating and applying operational risk control measures to prepare for potential crisis events.

References

- Acharya, V.V. and Steffen, S. 2020. The risk of being a fallen angel and the corporate dash for cash in the midst of Covid. *The Review of Corporate Finance Studies*, 9(3); 430-471. Available at: <https://academic.oup.com/rcfs/article/9/3/430/5879284> (Accessed on 15 March 2022).
- Ahmad, A., Muhammad, M. and Narullia, D. 2021. Corporate risk disclosure: The effect of corporate governance. *Journal of Applied Managerial Accounting*, 5(1); 101-113. Available at: https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Ahmad%2C+A.%2C+Muhammad%2C+M.+and+Narullia%2C+D.+2021.+Corporate+risk+disclosure%3A+The+effect+of+corporate+governance.+&btnG= (Accessed on 28 April 2022)
- Ajayi, V.O. 2017. Primary sources of data and secondary sources of data. *Benue State University*, 1(1); 1-6.
- Akanle, O., Adesina, J.O. and Akarah, E.P. 2016. Towards human dignity and the internet: The cyber-crime phenomenon in Nigeria. *African Journal of Science, Technology, Innovation and Development*, 8(2); 213-220. Available at: <https://journals.co.za/doi/abs/10.1080/20421338.2016.1147209> (Accessed on 12 October 2022).
- Alberts, C.J. and Dorofee, A.J. 2010. Risk management framew. *Carnegie-Mellon Univ Pittsburgh PA Software Engineering Institute*.
- Al-Harbi, A. 2019. The determinants of conventional banks profitability in developing and underdeveloped countries. *Journal of Economics, Finance and Administrative Science*, 24(47); 4-28. Available at: <https://www.emerald.com/insight/content/doi/10.1108/JEFAS-05-2018-0043/full/html> CrossRef. ISSN 2077-1886. DOI 10.1108/JEFAS-05-2018-0043 (Accessed on 25 May 2023).
- Alghazo, J.M., Kazmi, Z. and Latif, G. 2017. Cyber-security analysis of internet banking in emerging countries: User and bank perspectives. *International Conference on Engineering Technologies and Applied Sciences*, 4(1). Available at: <https://ieeexplore.ieee.org/abstract/document/8277910>. (Accessed on 11 March 22).
- Amirrudin, M., Nasution, K. and Supahar, S. 2021. Effect of variability on Cronbach alpha reliability in research practice. *Journal Matematika, Statistika dan Komputasi*, 17(2); 223-230. Available at: <http://journal.unhas.ac.id/index.php/jmsk/article/view/11655>. (Accessed on 22 May 2023)

Andrieș, A.M., Căpraru, B. and Nistor, S. 2018. Corporate governance and efficiency in banking: evidence from emerging economies. *Applied Economics*, 50(34-35).3812-3832. Available at: <https://search.proquest.com/docview/2043188161> CrossRef. ISSN 0003-6846. DOI 10.1080/00036846.2018.1436144 (Accessed on 25 May 2023).

Anton, S.G. and Nucu, A.E.A. 2020, Enterprise risk management: A literature review and agenda for future research. *Journal of Risk and Financial Management*, 13(11); 281. Available at: <https://www.mdpi.com/1911-8074/13/11/281>. (Accessed on 16 September 2023)

Ashraf, B.N. and Goodell, J.W. 2022. Covid-19 social distancing measures and economic growth: Distinguishing short-and long-term effects. *Finance Research Letters*, 47; 102639. Available from: <https://www.sciencedirect.com/science/article/pii/S1544612321005742>. (Accessed on 28 December 2022).

Apostolik, R., Donohue, C. and Went, P. 2009. *Foundations of banking risk: An overview of banking, banking risks, and risk-based banking regulation*. (s.l.): John Wiley.

Apuke, O.D. 2017. Quantitative research methods: A synopsis approach. *Kuwait Chapter of Arabian Journal of Business and Management Review*, 33(5471); 1-8. Available at: <https://platform.almanhal.com/Files/Articles/107965>. Accessed on 10 June 2021).

Arduini, F. and Morabito, V. 2010. Business continuity and the banking industry. *Communications of the ACM*, 53 (3); 121-125. Available at:<https://dl.acm.org/doi/abs/10.1145/1666420.1666452>. (Accessed on 15 July 2022).

Alturki, R. 2021. Research onion for smart IoT-enabled mobile applications. *Hindawi Scientific Programming*. 9. Available at: <https://doi.org/10.1155/2021/4270998> (Accessed on 11 June 2023).

Bahamid, R.A. and Doh, S.I. 2017. A review of risk management process in construction projects of developing countries. *IOP Conference Series. Materials Science and Engineering*, 271(1); 12042. Available at: <https://iopscience.iop.org/article/10.1088/1757-899X/271/1/012042> CrossRef. ISSN 1757-8981. DOI 10.1088/1757-899X/271/1/012042 (Accessed on 24 April 2023).

Baker, H.K., Filbeck, G., Holzhauser, H., Saadi, S. and Christian-Ioan Tiu, C.I. 2015. Risk management: A panel discussion. *Journal of Applied Finance*, 25(1); 46-57.

Baldwin, R. and Di Mauro, B.W. 2020. Economics in the time of Covid-19: VOX CEPR Policy Portal (A new eBook). Available at: <https://fondazionecerm.it/wp->

content/uploads/2020/03/CEPR-Economics-in-the-time-of-COVID-19 -A-new-eBook.pdf.

(Accessed on September 2022).

Basel Committee of Banking Supervision. 2010. *Sound Practices for the Management and Supervision of Operational Risk*. Bank for International Settlements.10; 1-26. Available at:

<http://www.bis.org/publ/bcbsr292.htm>. (Accessed on 20 January 2022)

Basel Committee on Banking Supervision. 2006. International convergence of capital measurement and capital standards a revised framework comprehensive version. *Bank for International Settlements*, 1- 333. Available at: <http://www.bis.org/publ/bcbsr292.htm>.

(Accessed on 02 October 2022)

Basel Committee on Banking Supervision. 2020. Review of the principles for sound management of operational risk. *Bank of international Settlements*. Available at:

<http://www.bis.org/publ/bcbsr292.htm>. (Accessed on 04 January 2023)

Basel Committee on Banking Supervision. 2018. SRP Supervisory review process SRP30 Risk management, 12-15. Available at:

<https://static1.squarespace.com/static/651aef81e460f47f052567f7/t/653bc441caf6fd0d68da1569/1698415682026/BIS+Basel+Framework-Banking+Risk.pdf>.

(Accessed on 03 February 2022)

Basel Committee on Banking Supervision. 2021. Revisions to the principles for the sound management of operational risk. *Bank of International Settlements*, 1-23. Available at:

<https://static1.squarespace.com/static/651aef81e460f47f052567f7/t/653bc441caf6fd0d68da1569/1698415682026/BIS+Basel+Framework-Banking+Risk.pdf>. (Accessed on 20 March 2022)

Berg, V.D, M.J., Bhatt, D.L., Kappelle, L.J., De Borst, G.J., Cramer, M.J., Van Der Graaf, Y., Steg, P.G. and Visseren, F.L. 2017. Smart study group and reach registry investigators, identification of vascular patients at very high risk for recurrent cardiovascular events: validation of the current ACC/AHA very high risk criteria. *European Heart Journal*, 38(43); 3211-3218. Available at: <https://academic.oup.com/eurheartj/article/38/43/3211/3092058>.

(Accessed on 28 August 2021).

Berg, A.Z. 2002. Firearms risk management. *Psychiatric Services*, 53 (4); 482-483. Available at: <https://ps.psychiatryonline.org/doi/full/10.1176/appi.ps.53.4.482-a>. (Accessed on 02 May 2022).

Bitar, M. and Tarazi, A. 2022. A note on regulatory responses to Covid-19 pandemic: Balancing banks' solvency and contribution to recovery. *Journal of Financial Stability*, 60; 101009. Available at:

<https://www.sciencedirect.com/science/article/pii/S1572308922000365>. (Accessed on 18 December 2022).

Bloomberg News. 2014. Abil hit risks R4bn in the state pension. *Business report*. Available from:

<https://bristoluniversitypressdigital.com/display/book/9781447326656/ch006.xml>. (Accessed on 06 July 2022).

Bloomfield, J. and Fisher, M.J. 2019. Quantitative research design. *Journal of the Australian Political economy*, 22(2), 27-30. Available at:

<https://search.informit.org/doi/abs/10.3316/INFORMIT.738299924514584>. (Accessed on 13 February 2022).

Blunden, T. and Thirlwell, J. 2013. *Mastering operational risk: A practical guide to understanding operational risk and how to manage it*. 3rd ed. Edinburg Gate: Pearson. UK.

Bonett, D.G. and Wright, T.A. 2015. Cronbach's alpha reliability: Interval estimation, hypothesis testing, and sample size planning. *Journal of Organizational Behavior*, 36 (1), 3-15. Available at: <https://onlinelibrary.wiley.com/doi/abs/10.1002/job.1960>. (Accessed on 13 April 2022).

Boin, A. and Hart, P. 2010. Organising for effective emergency management: Lessons from research 1. *Australian Journal of public administration*, 69 (4); 357-371. Available at: <https://api.istex.fr/ark:/67375/WNG-J4S65V5K-Q/fulltext.pdf> *International Bibliography of the Social Sciences (IBSS)*. ISSN 0313-6647. DOI 10.1111/j.1467-8500.2010.00694.x. (Accessed on 17 January 2023).

Bryman, A. Bell, E., Hirschsohn, Santos, D. and Toit, D. 2014. *Research Methodology: Business and Management Contexts*, Oxford University Press Southern Africa (Pty) Limited.

Bryman, A. and Bell, E. 2011. *Business research methods*. 3rd ed. New York: Oxford University Press.

Craigen, D., Diakun-Thibault, N. and Purse, R. 2014. Defining cyber-security. *Technology Innovation Management Review*, 4 (10). Available at: <https://www.timreview.ca/article/835>. (Accessed on 23 January 2022.).

Carretta, A., Farina, V. and Schwizer, P. 2017. Risk culture and banking supervision. *Journal of Financial Regulation and Compliance*, 25 (2); 209-226. Available

from: <https://www.emerald.com/insight/content/doi/10.1108/JFRC-03-2016-0019/full/html> CrossRef. ISSN 1358-1988. DOI 10.1108/JFRC-03-2016-0019. (Accessed on 20 September 2022).

Central Bank of Lesotho. 2018. Annual report. Maseru. Available at: <http://www.centralbank.org.ls>. (Accessed on 12 May 2021).

Central Bank of Lesotho. 2020. Annual Report. Maseru. Available at: <http://www.centralbank.org.ls>. (Accessed on 10 March 2022).

Central Bank of Lesotho. 2020. Financial stability report. Maseru. Available at: <http://www.centralbank.org.ls>. (Accessed on 11 May 2021).

Central Bank of Lesotho. 2020. Newsletter. Maseru. Available at: <http://www.centralbank.org.ls>. (Accessed on 16 June 2021).

Central Bank of Lesotho. 2020. Supervision report. Maseru. Available at: <http://www.centralbank.org.ls>. (Accessed from 15 September 2021).

Central Bank of Lesotho. 2020. Payment systems and settlements report. Maseru. Available at: <http://www.centralbank.org.ls>. (Accessed on 22 April 2021).

Chapman, R.J., 2011. *Simple tools and techniques for enterprise risk management*. 2nd ed. Chichester: Wiley.

Chisasa, J. and Young, J., 2013. Implementing a Risk Management Framework in Developing Markets. *The International Business & Economics Research Journal*, 12(6), 603. Available at: <https://search.proquest.com/docview/1418721277> CrossRef. ISSN 1535-0754. DOI 10.19030/iber.v12i6.7867. (Accessed on 21 October 2021).

Chung, C. and Zhu, H. 2021. Corporate governance dynamics of political tie formation in emerging economies: Business group affiliation, family ownership, and institutional transition, corporate governance. *An International Review*, 29(4); 381-401. Available at: <https://onlinelibrary.wiley.com/doi/abs/10.1111/corg.12367>. (Accessed on 10 May 2022).

Çolak, G. and Öztekin, Ö 2021. The impact of Covid-19 pandemic on bank lending around the world. *Journal of Banking and Finance*, 133. Available at: [106207](https://doi.org/10.1016/j.jbf.2021.106207). CrossRef. ISSN 1556-5068. DOI 10.2139/ssrn.3712668. (Accessed on 20 April 2023).

Coleman, R., 2011. *Operational risk*. Hoboken, NJ, USA: John Wiley and Sons, Inc, Jan 07, Available at: <https://onlinelibrary.wiley.com/doi/abs/10.1002/9780470400531.eorms0591> DOI 10.1002/9780470400531.eorms0591. (Accessed on 04 March 2023).

Collis, J. Hussey, R. 2014. *Writing up the research. In business research*; Springer: Berlin/Heidelberg, Germany.

Cooper, D.R. and Schindler, P. 2008. *Business research methods*, McGraw-Hill. <https://scholar.google.com>.

COSO (The Committee of Sponsoring Organizations of the Treadway Commission). 2009. Enterprise risk management. Integrated framework: Executive summary. Available at: <https://www.coso.org/Documents/COSO-ERM-Executive-Summary>. (Accessed on 15 March 2022)

COSO (The Committee of Sponsoring Organizations of the Treadway Commission). 2012. Enterprise risk management: Understanding and communicating risk appetite. Available at: <https://www.coso.org/Documents/ERM-Understanding-and-Communicating-Risk-Appetite>. (Accessed on 22 May 2022).

Correia, C., Flynn, U., E., Wormald, M. and Dion, J. 2015. *Financial management* 8th ed. Juta and company (Pty) Ltd.

Chhabra, N. 2013. Risk management in banking sector: International journal of marketing. *Financial Services and Management Research*, (2) 2.

Creswell, J.W. 2009. *Research design: Qualitative, quantitative and mixed methods approaches*, 3rd ed. California: SAGE publications, Inc.

Creswell, J.W. 2014. *A concise introduction to mixed methods research*. Washington DC: SAGE publication.

Creswell, J.W. and Creswell, J.D., 2023. *Research design*. 6th edition. Thousand Oaks; SAGE Publications ISBN 1071870637.

Dermine, J., 2013. Bank corporate governance, beyond the global banking crisis. *Financial Markets, Institutions and Amp; Instruments*, (5); 259-281. Available at: <https://api.istex.fr/ark:/67375/WNG-Q9XVG1RJ-C/fulltext.pdf> International Bibliography of

[the Social Sciences \(IBSS\). ISSN 0963-8008. DOI 10.1111/fmii.12012.](#) (Accessed on 20 June 2022).

De Villis, R. 2011. *Scale Development: Theory and application*: Los Angeles, Sage Publications.

Du Randt, R. 2011. *Risk management for banks: Study guide for RSK1501*. Pretoria: University of South Africa.

Eichenbaum, M.S., Rebelo, S. and Trabandt, M. 2022, Inequality in life and death. *IMF Economic Review*, 1-37. Available from: <https://link.springer.com/article/10.1057/s41308-021-00147-3>. (Accessed on 25 January 2023).

Ehiedu, V.C. 2022, Analysis of micro prudential determinants of capital adequacy in deposit money banks. *International Journal of Management and Entrepreneurship Research*, 4(11); 398-415. Available at: <https://doi.org/10.51594/ijmer.v4i11.393>. (Accessed on 26 May 2020)

Epetimehin, F.M. and Obafemi, F. 2015. Operational risk management and the financial sector development: An overview. *International Journal of Economics, Commerce and Management. United Kingdom*, 3 (3); 1-11. Available at: <http://ijecm.co.uk/>. ISSN 2348 0386. (Accessed on 02 June 2022)

European Investment Fund. 2010. Operational Risk Management. 2010:5. Available at: http://www.eif.org/news_centre/publications/operational_risk_management_charter. (Accessed on 12 June 2021)

Federal Reserve Bank. 2016. Interest rate management at community banks-community banking connections. 1-9.

Financial Stability Board. 2014. Guidance on supervisory interaction with financial institution on risk culture: A framework for assessing risk culture.

Frigo, M.L. and Anderson, R.J. 2011. What is strategic risk management? *Strategic Finance*, 92(10); 21.

Gjerdrum, D. and Peter, M. 2011. The new international standard on the practice of risk management—A comparison of ISO 31000: 2009 and the COSO ERM framework. *Risk Management*, 31(21); 8-12. Available at: <https://www.soa.org/globalassets/assets/Library/newsletters/risk-management-newsletter/2011/march/jrm-2011-iss21-gjerdrum.pdf>. (Accessed on 30 May 2023).

Girling, P.X. 2022, *Operational Risk Management: A Complete Guide for Banking and Fintech*, John Wiley and Sons. Available at: <https://library.biblioboard.com/viewer/3ec982df->

[158a-4fc9-8136-95f7cc81d5d8](#) ISBN 1118532457. DOI 10.1002/9781118755754. (Accessed on 25 May 2023).

Gonda, X. and Tarazi, F.I. 2022. Well-being, resilience and post-traumatic growth in the era of Covid-19 pandemic. *European Neuropsychopharmacology*, 54; 65-66. Available at: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8413303/>. (Accessed on 20 March 2023).

Hakenes, H. and Schnabel, I. 2010. Credit risk transfer and bank competition. *Journal of Financial Intermediation*, 19(3); 308-332. Available at: <https://www.sciencedirect.com/science/article/abs/pii/S1042957310000069>. (Accessed on 17 April 2022).

Harner, M.M. 2010. Barriers to effective risk management, 40; 1323. Available at: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/shlr40&div=43&id=&page=>. (Accessed on 18 August 2022).

Huy, D.T.N., Thach, N.N., Chuyen, B.M., Nhung, P.T.H., Tran, D.T. and Tran, T.A. 2021. Enhancing risk management culture for sustainable growth of Asia commercial bank-ACB in Vietnam under mixed effects of macro factors. *Entrepreneurship and Sustainability Issues*, 8 (3); 291. Available at: [http://doi.org/10.9770/jesi.2021.8.3\(18\)](http://doi.org/10.9770/jesi.2021.8.3(18)). (Accessed on 23 January 2022).

Harvey, G.E. 2012. The process of risk management: important steps to take. *Petroleum Accounting and Financial Management Journal*, 31(1); 77. Available at: <https://www.proquest.com/openview/c4f4af98f65b01948c35ac4f525c23e1/1?pq-origsite=gscholar&cbl=30591>. (Accessed on 20 September 2022).

Hassan, A.B., Lass, F.D. and Makinde, J. 2012. Cyber-crime in Nigeria: Causes, effects and the way out. *Journal of Science and Technology*, 2(7); 626-631. Available at: http://www.ejournalofscience.org/archive/vol2no7/vol2no7_11.pdf Accessed on 11 March 2023).

Heffernan, S. 2005. *Modern Banking*. Chichester: Wiley

Helbok, G. and Wagner, C. 2006. Determinants of operational risk reporting in the banking industry. *The Journal of Risk Management*, 9(1); 49-74. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=425720. (Accessed on 17 September 2022).

Hendrikse, J.W. and Hefer-Hendrikse, L. 2012. *Corporate governance handbook: Principles and practices*. 2nd ed. Kenwyn, South Africa: Juta.

Henderson KA 2011. Post-positivism and the pragmatics of leisure research. *Leisure Sciences. An Interdisciplinary Journal*, 33(4); 341-346. Available at:

<https://www.tandfonline.com/doi/abs/10.1080/01490400.2011.583166>. (Accessed on 30 October 2023).

Hundal, G. and Zinakova, S. 2021. Financial technology in the finish banking baking sector and its impact on stakeholders in the wake of covid-19: Risk governance and control financial markets and institutions.11 (1). Available at: <https://www.theseus.fi/handle/10024/504108>. (Accessed on 30 May 2022).

International Monetary Fund (IMF). 2020. Corporate Funding and Covid-19 Crises.

The Institute of Operational Risk (IOR). 2011. Risk appetite. Institute of Operational Risk sound practice guidance. Available at: <https://www.ior-institute.org/sound-practice-guidance/operational-risk-appetite-and-tolerance/> (Accessed on 23 May 2022)

The Institute of Operational Risk (IOR). 2016. Embedding an operational risk management framework. Institute of Operational Risk sound practice guidance paper. Available at <https://www.ior-institute.org/sound-practice-guidance/embedding-an-operational-risk-management-framework> (Accessed on 23 May 2022)

Institute of Operational Risk Management (IOR). 2019. Operational Resilience. Operational risk sound practice guidance. Available at: <https://www.ior-institute.org/sound-practice-Operational-risk-sound-practice-guidance>. (Accessed on 04 March 2022).

Information systems audit and control association (ISACA). 2005. IS Auditing Guideline: G32 Business Continuity Plan Review from IT Perspective.

Information systems audit and control association (ISACA). 2010. Social media: Business benefits and security, Governance and assurance perspective.

Information systems audit and control association (ISACA). 2011. Business Continuity Management Audit/Assurance Programme.

International Standards of Organizations (ISO). 2009. ISO 31000: Risk management – Principles and guidelines. ISO 31000:2009(E). Available at: <http://ehss.moe.gov.ir/getattachment/56171e8f-2942-4cc6-8957-359f14963d7b/ISO-31000>. (Accessed on 16 June 2022).

Isoh, A.V.N. and Nchang, N.D. 2020. Assessing the impact of operational risk management on Financial Performance of Selected Mainstream Commercial Banks in Cameroon. *International journal of research in commerce and management studies*. 2(2); 1-

16. Available at: (ISSN: 2582-2292), <https://pdfs.semanticscholar.org/ad74/2e661705d88fd07f53f5082f48266ab98987.pdf>.

(Accessed on 17 May 2022).

Jednak, D. and Jednak, J. 2013. Operational Risk Management in Financial Institutions. *Management (Belgrade university, faculty of organizational sciences)*, 18(66); Available at: [71-80 CrossRef. ISSN 1820-0222. DOI 10.7595/management.fon.2013.0004](#). (Accessed on 16 July 2020).

Johnson, J.M. and Khoshgoftaar, T.M. 2020. The effects of data sampling with deep learning and highly imbalanced big data. *Information Systems Frontiers*, 22(5); 1113-1131. Available at: <https://link.springer.com/article/10.1007/s10796-020-10022-7>. (Accessed on 29 September 2022).

Kaka, E.J. 2021. Covid-19 and Auditing. *Journal of Applied Accounting and Taxation*, 6(1); 1-10. Available at: <https://journal.polibatam.ac.id/index.php/JAAT/article/view/2311>. (Accessed on 16 July 2023).

Kanchu, T. and Kumar, M.M. 2013. Risk management in banking sector—an empirical study. *International journal of marketing, financial services and management research*, 2(2); 145-153. Available at: DOI: [10.4236/jfrm.2019.82005](#) (Accessed on 14 January 2022).

Kaplan, G.E. 2004. Do governance structures matter? *New Directions for Higher Education*, 127.23-34. Available at: <https://api.istex.fr/ark:/67375/WNG-TJ511R0B-3/fulltext.pdf> ERIC. ISSN 0271-0560. DOI [10.1002/he.153](#). (Accessed on 27 April 2023).

Kesharwani, A. and Tripathy, T. 2012. Dimensionality of perceived risk and its impact on internet banking adoption: an empirical investigation. *Services Marketing Quarterly*, 33(2); 177-193. Available at: <https://www.tandfonline.com/doi/abs/10.1080/15332969.2012.662461>. (Accessed on 28 April 2023).

Kesharwani, S., Sarkar, M.O. and Oberoi, S. 2019. Growing thread of cyber-crime in indian banking sector, 1(4).19-22. Available at: <https://cybernomics.in/index.php/cnm/article/view/73>. (Accessed on 10 July 2022).

Ketefian, S. 2015. Ethical considerations in research. Focus on vulnerable groups, *Investigación y Educación en Enfermería*, 33(1); 164-172.

Kisa, Ö. 2020. The Impact of the Pandemic on the Banking Sector and Some Policy Recommendations.

Kivunja, C. and Kuyini, A.B. 2017. Understanding and applying research paradigms in educational contexts. *International Journal of higher education*, 6(5); 26-41. Available at: <https://eric.ed.gov/?id=EJ1154775>. (Accessed on 16 June 2023).

Khalilzadeh, M., Katouezadeh, L. and Zavadskas, E.K., 2020. Risk identification and prioritization in banking projects of payment service provider companies: an empirical study. *Frontiers of Business Research in China*, 14(2); 145-171. Available from: <https://journal.hep.com.cn/fbr/EN/10.1186/s11782-020-00083-5> CrossRef. ISSN 1673-7326. DOI 10.1186/s11782-020-00083-5. (Accessed on 11 November 2021)

Khan, M.J., Hussain, D. and Mehmood, W. 2016. Why do firms adopt enterprise risk management (ERM)? Empirical evidence from France. *Management Decision*, 54(8); 1886-1907. Available at: <https://www.emerald.com/insight/content/doi/10.1108/MD-09-2015-0400/full/html>. (Accessed on 10 January 2022).

Kimball, A.L. 2023. Support for a risk management model of institutional burdens in beyond 2%—NATO Partners, Institutions and Burden Management: Concepts, Risks and Models Springer; 133-196. Available at: https://link.springer.com/chapter/10.1007/978-3-031-22158-3_7. (Accessed on 28 October 2023).

Korzeb, Z. and Niedziółka, P. 2020. Resistance of commercial banks to the crisis caused by the Covid-19 pandemic: the case of Poland, Equilibrium. *Quarterly Journal of Economics and Economic Policy*, 15 (2); 205-234. Available at: <https://www.cceol.com/search/article-detail?id=898620>. (Accessed on 19 August 2023).

Kulpa, W. and Magdon, A. 2012. Operational risk management in a bank. *Internal Auditing and Risk Management*, 7(4); 35-50.

Kumar, P. and, J. 2020. Impact of Covid-19 on Higher Education in India. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3691541. (Accessed on 20 September 2022).

Kumar, R. 2011. *Research methodology: A step-by-step guide for beginners*. 3rd ed. SAGE Publications Ltd: London.

Khrawish, H.A. 2011. Determinants of commercial banks performance: Evidence from Jordan, *International Research Journal of Finance and Economics*, 81(1); 148-159.

Lagoarde-Segot, T. and Leoni, P.L. 2013. Pandemics of the poor and banking stability, *Journal of Banking & Finance*, 37(11); 4574-4583. Available at: <https://www.sciencedirect.com/science/article/abs/pii/S0378426613001878>. (Accessed on 10 August 2022).

Lai, F., Shad, M.K., Khan, A.A., Kashif Shad, M. and Ali Khan, A. 2017. Value Creating Determinants of enterprise risk management and its economic value added. *European Proceedings of Social and Behavioural Sciences*, 44. Available at: DOI 10.15405/epsbs.2018.07.02.75. (Accessed on 12 June 22)

Lallie, H.S., Shepherd, L.A., Nurse, J.R.C., Erola, A., Epiphaniou, G., Maple, C. and Bellekens, X. 2021. Cyber-security in the age of Covid- 19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic, *Computers and Amp; Security*, 105; 102248. Available at: <https://www.sciencedirect.com/science/article/pii/S0167404821000729>. (Accessed on 01 June 2022).

Leedy. P.D and Ormrod, J. 2010. *Practical Research – Planning and Design*. 9th ed. Merrill: Pearson Education, Inc.

Li, X., Feng, H., Zhao, S. and Carter, D.A. 2021. The effect of revenue diversification on bank profitability and risk during the Covid-19 pandemic, *Finance Research Letters*, 43; 101957. Available at: <https://www.sciencedirect.com/science/article/pii/S1544612321000386>. (Accessed on 20 April 2022).

Louw, L and Venter, P 2013. *Strategic management, developing sustainability in Southern Africa*. 4th ed. South Africa: Oxford University Press.

Mahendra, P.A., Pitroda, J.R. and Bhavsar, J.J. 2013. A study of risk management techniques for construction projects in developing countries. *International Journal of Innovative Technology and Exploring Engineering*, 3(5);139-142. Available at: <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=38da30dd224c3ad241d12c62b56298b406d95fa4>. (Accessed on 20 March 2022).

Manjikian, M. 2013. Positivism, post-positivism, and intelligence analysis. *International Journal of Intelligence and Counterintelligence*, 26 (3); 563-582. Available at: <https://doi.org/10.1080/08850607.2013.758002> (Accessed on 30 May 2023)

Marcinkowska, M., Szambelańczyk, J., Szambelańczyk, J.P. and PI Ewa Kulińska-Sadłocha. 2020. The impact of pandemic risk on the activity of banks based on the Polish banking sector in the face of Covid-19. Available at: <https://scholar.google.com/scholar>. (Accessed on 11 June 2022).

Mare, S. 2019. Principles for an operational framework for a bank: A *South African perspective*. MCom dissertation. University of South Africa.

Marinoni, G., Van, Land, H. and Jensen, T. 2020. The impact of covid-19 on higher education around the world. *Global Survey Report*. Available at: https://www.uniss.it/sites/default/files/news/iau_covid19_and_he_survey_report_final_may_2020.pdf. (Accessed on 11 August 2022).

Matlanyane, A. and Harmse, C. 2002. Revenue implications of trade liberalization in South Africa. *The South African Journal of Economics*, 70(2); 155-161. Available at: <https://repository.up.ac.za/handle/2263/5565>. (Accessed on 10 January 2022).

Mishra, N.P., Das, S.S., Yadav, S., Khan, W., Afzal, M., Alarifi, A., Kenawy, E., Ansari, M.T., Hasnain, M.S. and Nayak, A.K. 2020. Global impacts of a pre-and post-Covid-19 pandemic: Focus on socio-economic consequences. *Sensors International*, 1; 100042. Available at: <https://www.sciencedirect.com/science/article/pii/S2666351120300425>. (Accessed on 26 January 2023).

Moosa, I.A. 2007. *Operational Risk Management*. New York: Palgrave Macmillan.

Moore, S., Neville, C. and Murphy, M. 2010. *The ultimate study skills handbook*, London: McGraw-Hill Education.

Mu, J., Peng, G. and Maclachlan, D.L., 2009. Effect of risk management strategy on NPD performance. *Technovation*, 29 (3);170-180. Available at: <https://dx.doi.org/10.1016/j.technovation.2008.07.006> CrossRef. ISSN 0166-4972. DOI 10.1016/j.technovation.2008.07.006. (Accessed on 22 November 2022).

Muhsyaf, S.A., Cahyaningtyas, S.R. and Sasanti, E.E. 2021. Three line of defence: Effective risk management. *Advances in Economics and Management Research*, 180; 85-91. Available from: <http://eprints.unram.ac.id/39383/>. (Accessed on 19 May 2022).

Myers, J.L., Arnold, D.W., Robert, F. and Lorch, JR. 2010. *Research design and statistical analysis*. 3rd ed. New York: Routledge

Naciti, V., Cesaroni, F. and Pulejo, L., 2021. Corporate governance and sustainability: a review of the existing literature. *Journal of Management and Governance*, 26(1);55-74. Available at: <https://link.springer.com/article/10.1007/s10997-020-09554-6> CrossRef. ISSN 1385-3457. DOI 10.1007/s10997-020-09554-6. (Accessed on 22 November 2022).

Nicolini, G., Gärling, T., Carlander, A. and Hauff, J.C. 2017. Attitude toward risk and financial literacy in investment planning. *Springer International Publishing*, 1-10. Available at: [DOI 10.1007/978-3-319-57592-6_14](https://doi.org/10.1007/978-3-319-57592-6_14). (Accessed on 26 May 2021).

North Caroline Banking Institution, 2021. The Brick and Mortar Bank is dead-Covid-19 killed it. Analysing the new normal for data security in the increasingly digital financial service industry. Available at:

<https://heinonline.org/HOL/LandingPage?handle=hein.journals/ncbj25&div=14&id=&page=>.

(Accessed on 17 February 2023).

OECD (Organisation for economic cooperation and development), 2009. The OECD (Q)SAR Application Toolbox. Available at:

http://www.oecd.org/document/12/0,3343,en_2649_34379_42930060_1_1_1_1,00.html.

(Accessed on July 18 2021).

Olaekan, A. and Adeyinka, S. 2013. Capital adequacy and banks' profitability: An empirical evidence from Nigeria. *American International Journal of Contemporary Research*, 3(10); 87-93. Available at: <https://www.calebuniversity.edu.ng/oer/storage/2022/03/13-8d960c8e.pdf>.

(Accessed on 29 May 2021).

Olasanmi, O.O., 2010. Computer crimes and counter measures in the Nigerian banking sector. *Journal of Internet Banking and Commerce*. 15(1); 1-10. available at:

[https://www.proquest.com/openview/0382003467356cf59096860047fff021/1?pq-](https://www.proquest.com/openview/0382003467356cf59096860047fff021/1?pq-origsite=gscholar&cbl=39255)

[origsite=gscholar&cbl=39255](https://www.proquest.com/openview/0382003467356cf59096860047fff021/1?pq-origsite=gscholar&cbl=39255). (Accessed on 06 January 2022).

Oluwaseyi, Ebernezer, O., Ahmad, W. and Omar, B. 2016. Risk Management and the Financial Performance of Commercial Banks in Nigeria: A Literature Review Revisited.

Available at: <https://smartlib.umri.ac.id/assets/uploads/files/a9c7a-c0702031419.pdf>.

(Accessed on 27 February 2022).

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

Onwuegbuzie, A.J., Leech, N.L and Collins, K.M.T. 2012. Quantitative analysis technique for review of literature.17 (56); 1-28. Available at: <https://eric.ed.gov/?id=EJ981457>. (Accessed on 11 September 2023).

Ozilli, P. and Arun, T. 2020. Spillover of covid-19: Impact on the global economy.1-27. Academic press.

Panwar, A.H., Ansari, S. and Shah, A.A. 2017. Post-positivism: an effective paradigm for social and educational research. *International Research Journal of Arts and Humanities*, 45;

8-26. Available at: <https://www.researchgate.net/profile/Dr-Abdul-Hameed-> (Accessed on 21

May 2023).

Parker, R. and Bradley, L. 2000. Organisational culture in the public sector: evidence from six organisations, *International Journal of Public Sector Management*, 13 (2); 125-141. Available at:

<https://www.emerald.com/insight/content/doi/10.1108/09513550010338773/full/html>.

(Accessed on 03 February 2022).

Plachkinova, M. 2021. Exploring the Shift from Physical to Cyber-crime at the Onset of the Covid-19 Pandemic, *International Journal of Cyber Forensics and Advanced Threat Investigations*, 2 (1); 50-62. Available at:

<https://www.conceptchint.net/index.php/CFATI/article/view/29>. (Accessed on 18 March 2022).

Phillips, D.C. and Burbules, N.C. 2009. *Postpositivism and educational research: Philosophy, theory, and educational research series*. Maryland: Rowman and Littlefield Publishers, Inc.

Ponto, J. 2015. Understanding and evaluating survey research, *Journal of the Advanced Practitioner in Oncology*, 6 (2); 168. Available at:

<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4601897/>. (Accessed on 30 April 2022).

Prewett, K. and Terry, A. 2018. COSO's Updated Enterprise Risk Management Framework: A quest for depth and clarity. *The Journal of Corporate Accounting and Amp*. 29(3) 16-23. Available at:

<https://onlinelibrary.wiley.com/doi/abs/10.1002/jcaf.22346> CrossRef. ISSN 1044-8136. DOI 10.1002/jcaf.22346 (Accessed on 23 September 2021).

Price Water Coopers (PWC). 2021. It is to Reimagine where and how work will get done. PWC Website. Available at: <https://www.pwc.com/us/en/library/covid-19/us-remote-work-survey.html> (Accessed on 18 May 2023)

Ramasamy, K. 2020. Impact analysis in banking, Insurance and financial service industry due to covid-19 Pandemic: *Pramana Research Journal*. Available at:

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3668165. (Accessed on 19 June 2023).

Rehman, A.A. and Alharthi, K. 2016. An introduction to research paradigms. *International Journal of Educational Investigation*, 3 (8); 51-59. Available at:

<https://www.ijeionline.com/attachments/article/57/IJEI.Vol.3.No.8.05.pdf>. (Accessed on 28 September 2-23).

Richard, F.D., Bond, C.F. and Stokes-Zoota, J.J. 2003. One Hundred years of social psychology quantitatively described: Review of general psychology, 7(4); 331-363.

Rouse, M. 2010. Definition: Enterprise Risk Management. Available at:

<http://searchcio.techtarget.com/definition/enterprise-risk-management>. (Accessed on 13 March 2022).

Roeschmann, A.Z., 2014. Risk Culture: What It Is and how It affects an insurer's risk management: *Risk Management and Insurance Review*, 17(2); 277-296. Available at: <https://api.istex.fr/ark:/67375/WNG-GQMJRJND-8/fulltext.pdf> ISSN 1098-1616. DOI 10.1111/rmir.12025. (Accessed 21 July 2021).

Rostami, A. 2016. Tools and techniques in risk identification: A research within SMEs in the UK Construction Industry. *Universal Journal of Management*, 4(4); 203-210. Available at: <https://search.proquest.com/docview/1945107563> CrossRef. ISSN 2331-950X. DOI 10.13189/ujm.2016.040406. (Accessed on 15 June 2022).

Ross, A. and Crossan, K. 2012. A review of the influence of corporate governance on the banking crises in the United Kingdom and Germany. *Corporate Governance*, 12(2); 215-225. Available at: <https://www.emerald.com/insight/content/doi/10.1108/14720701211214098/full/html> CrossRef. ISSN 1472-0701. DOI 10.1108/14720701211214098. (Accessed on 12 September 2022).

Salkind, N.J. 2019. *Exploring research*. 9th ed. Cape Town: Pearson.

Sarwar, A., Abdullah, M.I., Imran, M.K. and Fatima, T. 2023. When fear about health hurts performance: Covid-19 and its impact on employee's work. *Review of Managerial Science*, 17(2), 513-537. Available at: <https://link.springer.com/article/10.1007/s11846-022-00536-6>. (Accessed on 12 October 2023).

Saunders, A. and Cornett, M.M., 2008. *Financial institutions management*. 6th ed. New York: Pearson education.

Saunders, M., Lewis, P. and Thornhill, A. 2012. *Research methods for business students*. 6th ed. New York: Pearson education.

Saunders, M. and Tosey, P. 2013. *The layers of research design*. *Academia, Rapport*, Winter 2012/2013:58–59. Retrieved at: <http://www.academia.edu/4107831>. (Accessed on 10 January 2020).

Sekaran, U. and Bougie, R. 2013. *Research methods for business: A skill-building approach*. 6th ed. Chichester: Wiley.

Seliane, T.N. and Sello, M.N. 2015. The architecture of the Basel accords: perspectives on evolution and adoption in the context for Lesotho. Available at:

<https://centralbank.org.ls/images/Publications/Research/Papers/Occational/>. (Accessed on 10 January 2022).

Singleton, R.A. and Straits, B.C. 2009. Survey interviewing, *The SAGE handbook of interview research: The complexity of the craft*, 77-98.

Stead, E. and Smallman, C., 2014. Understanding Business Failure: Learning and Un-Learning from Industrial Crises. *Journal of Contingencies and Crisis Management*, (1); 1-18. Available at: <https://api.istex.fr/ark:/67375/WNG-8HGHRZRF-0/fulltext.pdf> CrossRef. SN 0966-0879. DOI 10.1111/1468-5973.00094. (Accessed on 10 October 2020).

Stanciu, L. and Stanciu, V. 2010. Grouped B-spline windows for the design of modulated filter banks anonymous. Available at: <https://ieeexplore.ieee.org/abstract/document/7528297>. (Accessed on 30 July 2022).

Sürücü, L. and Maslakci, A. 2020, "Validity and reliability in quantitative research, Business and Management Studies. *An International Journal*, 8(3); 2694-2726. Available at: <https://www.bmij.org/index.php/1/article/view/1540>. (Accessed on 14 September 2023).

Svata, V. and Fleischmann, M. 2011, Information security/Information technology risk Management in Banking Industry, *Acta Oeconomica Pragensia*, 19(3); 42—60.

Taheri, B., Porter, C., Valantasis-Kanellos, N. & König, C. 2015. Quantitative data gathering techniques. *Research Methods for Business and Management*, 4(14); 913-930. Available at: https://www.goodfellowpublishers.com/free_files. (Accessed on 10 October 2023).

Taherdoost. H. 2016. Validity and reliability of the research instrument: How to test the validation of a questionnaire/survey in research. *International Journal of Academic Research in Management (IJARM)*, 5. Available at:

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3205040. (Accessed on 16 September 2023).

Tamásné Vőneki, Z. 2020. Crisis management and operational risk management in the financial sector in the shadow of Covid-19. *Economy and Amp; Finance*, 7(3); 309-325. Available at: <https://real.mtak.hu/115837/1/309-325EVoneki.pdf>. (Accessed on 07 April 2022).

Tohidi, H. 2011. The role of risk management in IT systems of organizations. *Procedia Computer Science*, 3; 881-887.

The Hong Kong Institute of Bankers. 2013. *Operational risk management*. Hong Kong: John Wiley and Sons.

Thejane, R. 2017. The effect of asset liability management strategies and regulation on performance of commercial banks in Lesotho: Master of Management in Finance and Investment (MMFI) core view metadata. University of the Witwatersrand.

Usman, M., Cheng, J., Ghani, U., Gul, H. and Shah, W.U. 2023. Social support and perceived uncertainties during Covid-19: Consequences for employees' wellbeing, *Current Psychology (New Brunswick, N.J.)*, 42(12); 10248-10259. Available at:

<https://link.springer.com/article/10.1007/s12144-021-02293-3>. (Accessed on October 2023).

Valsamakis, A.C., Vivian, R.W., Du Toit, G.S. and Young, J. 2022. *Risk management*. 5thed. Sandton: Pearson. Available at: ISBN: 9781485711490 (Accessed on 30 April 2022).

Vanem, E. 2012. Ethics and fundamental principles of risk acceptance criteria. *Safety Science*, 50(4); 958-967. Available at: <https://dx.doi.org/10.1016/j.ssci.2011.12.030> CrossRef. ISSN 0925-7535. DOI 10.1016/j.ssci.2011.12.030. (Accessed on 12 April 2022).

Ugwuja, V.C., Ekunwe, P.A. and Henri-Ukoha, A. 2020. Cyber risks in electronic banking: exposures and cyber-security preparedness of women agro-entrepreneurs in South-South Region of Nigeria. *Journal of Business Diversity*, 20(3). Available at:

<https://articlearchives.co/index.php/JBD/article/view/1845>. (Accessed on 10 June 2022).

Wall, K.D. 2009. Thinking about risk: definition, assessment, and management: risk is present everywhere. Coping with risk is especially important in defence organizations. *The Armed Forces Comptroller*, 54 (3). 8.

Wang, W. and Envilov, M. 2020. The global impact of covid-19 on financial markets. Available at: [SSRN 3588021](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3588021). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3588021. (Accessed on 18 March 2022).

Wang, V., Nnaji, H. and Jung, J. 2020. Internet banking in Nigeria: Cyber-security breaches, practices and capability. *International Journal of Law, Crime and Justice*, 62(100415); 1-11. Available from: <https://www.sciencedirect.com/science/article/abs/pii/S1756061618303525>. (Accessed on 23 April 2022).

Wang, C., Cheng, Z., Yue, X. and McAleer, M. 2020. Risk management of Covid-19 by universities in China. *Journal of Risk and Financial Management*, 13 (2); 36. Available from: <https://www.mdpi.com/1911-8074/13/2/36>. (Accessed on 30 July 2023).

Wójcik, D. and Ioannou, S. 2020. Covid-19 and Finance: market developments so far and potential impacts on the financial sector and centres. *Tijdschrift voor economische en sociale geografie*, 111(3); 387-400. Available at:

<https://onlinelibrary.wiley.com/doi/full/10.1111/tesg.12434>. (Accessed on 05 February 2023).

World Health Organization (WHO), 2020. Novel Coronavirus disease 2019: situation report, 99. Available at:

<https://iris.who.int/bitstream/handle/10665/331909/nCoVsitrep28Apr2020-eng.pdf>. (Accessed on 24 September 2021).

Yang, S.O., Hsu, C., Sarker, S. and Lee, A.S. 2017. Enabling effective operational risk management in a financial institution: An action research study. *Journal of Management Information Systems*, 34(3);727-753. Available at:

<https://www.tandfonline.com/doi/abs/10.1080/07421222.2017.1373006>. (Accessed on 24 May 2021).

Yao, H., Haris, M. and Tariq, G. 2018. Profitability determinants of financial institutions. Available at: <https://www.mdpi.com/2227-7072/6/2/53>. (Accessed on 13 February 2021).

Yazdi, M. and Kabir, S. 2018. Fuzzy evidence theory and Bayesian networks for process systems risk analysis. *Human and Ecological Risk Assessment: An International Journal*. Available at: <https://www.tandfonline.com/doi/10.1080/10807039.2018.1493679>. (Accessed on 29 April 2023).

Young, J. 2009. Risk management for a typical petroleum, oil and gas company in South Africa. *Corporate Ownership and Control*, 6(4); 346-356. Available at:

<https://search.proquest.com/docview/37139434> CrossRef. ISSN 1727-9232. DOI 0.22495/cocv6i4c3p (Accessed on 26 August 2022).

Young, J. 2012. The use of key risk indicators by banks as an operational risk management tool: A South African perspective. *Corporate Ownership and Control*, 9(3); 172-185. Available at: [CrossRef](https://search.proquest.com/docview/37139434). ISSN 1727-9232. DOI 10.22495/cocv9i3c1art2 (Accessed on 20 October 2021).

Young, J. 2014. Practical guidelines to formulate an operational risk appetite statement for corporate organisations: A South African perspective. *Corporate Ownership and Control*, 12(1); 46-62. Available at:

<https://search.proquest.com/docview/1663903570> CrossRef. ISSN 1727-9232. DOI 10.22495/cocv12i1p3 (Accessed on 20 November 2021).

Young, J. 2015. Guiding criteria for operational risk reporting in a corporate environment. *Corporate Ownership and Control*, 13(1); 1241-1256.

<https://pdfs.semanticscholar.org/a26e/099a49da49b5bcfdf67fe481899e5bebc271.pdf>

(Accessed on 16 November 2021).

Young, J. 2018. Guiding criteria for an operational risk management framework for South African municipalities. *Administration publication*, 26(1); 9-41. Available at:

<https://journals.co.za/doi/abs/10.10520/ejc-adminpub-v26-n1-a2>. (Accessed on 15 October

2022).

Young, J. 2020. Determinants for a risk-based audit of an operational risk management framework: a South African perspective. *University of South Africa*, 24(7); 1-19 Available at:

<https://core.ac.uk/download/pdf/328838801.pdf>. (Accessed on 16 March 2022).

Young, J. 2022. *Operational risk management*. 3rd ed. Cape Town; Van Schaik.

Zawada, B. 2014. The practical application of ISO 22301. *Journal of Business Continuity and Emergency Planning*, 8 (1); 83-90. Available at:

<https://www.ingentaconnect.com/content/hsp/jbcep/2014/00000008/00000001/art00010>.

(Accessed on 15 May 2023).

Annexure A: Questionnaire

SURVEY										
OPERATIONAL RISK CONTROL MEASURES for the Lesotho Banking Industry to manage a crisis event: Case study of Covid-19 pandemic										
Aim										
The aim of the questionnaire is to confirm the importance of operational risk control measures that a bank should embed to effectively manage potential risks caused by a crisis event and to confirm the current status of these control measures in your organisation										
Introduction										
A literature review, based on an operational risk management framework, resulted in the identification of control measures that will allow an organisation to be prepared to effectively manage the potential consequences of a crisis event. The information gained from this questionnaire will assist in confirming effective operational risk controls, which Lesotho Banks can adopt to prepare for future crisis events. It is envisaged that the findings of this study will contribute towards the body of knowledge and the implementation of effective operational risk control measures.										
Confidentiality										
This survey is voluntary and all information will be regarded as confidential. No names will be linked to any feedback and data will be anonymous. You are, however, under no obligation to complete the survey and you can withdraw from the survey before submitting it. If you choose to participate in this survey, it will take no more than 15 minutes of your time. You will not directly benefit from your participation as an individual, but can add value towards the objective of this research.										
Time										
To complete the survey should take approximately 15 minutes										
Questions 1 to 4: Mark your answer with an X in the space provided										
Question 1					Question 2					
Indicate the department where you are employed		Answer			What is your focus area within the organisation?			Answer		
Top management					Business/Operations management					
Business management					Internal audit					
Financial management					Risk management					
Risk management					Compliance management					
Internal audit					Financial management					
Compliance management					Other:					
Other:										
Question 3					Question 4					
How many years experience do you have in risk management?		Answer			How many years experience do you have with your current organisation?			Answer		
0 – 1 year					0 – 1 year					
1 – 3 years					1 – 3 years					
3 – 5 years					3 – 5 years					
5 – 10 years					5 – 10 years					
More than 10 years					More than 10 years					
Answer the following by indicating an X in the appropriate space based on your knowledge and experience.										
Question 5										
A. To what degree do you rate the IMPORTANCE of the operational risk control measure that a bank should embed to effectively manage potential risks caused by a crisis event?										
B. To what extent do you agree that the operational risk control measures are CURRENTLY applicable as part of risk management in your organisation?										
CRITERIA	A. Your view on importance					B. Current applicability in your organisation				
	To no degree	To a lesser degree	To a moderate degree	To a degree	To a full degree	To no degree	To a lesser degree	To a moderate degree	To a degree	To a full degree
	1	2	3	4	5	1	2	3	4	5
1. Operational risk should be clearly defined and understood by all employees of the bank.										
2. An operational risk management framework should be embedded to serve as a platform to guide effective operational risk management.										
3. A risk culture should ensure the embedding of norms, attitudes and behaviours of employees relating to risk controls.										

4. A risk management strategy should be aligned with the business strategy to ensure that the objectives are within the set parameters of the risk appetite.										
5. A governance structure should be embedded to confirm the roles and responsibilities of role-players in risk management.										
6. A risk management process should be formalised and embedded in the organisation.										
7. Risk identification should be a step of an operational risk management process to identify the inherent risk exposures.										
	A. Your view on importance					B. Current applicability in your organisation				
8. Risk evaluation should be a step of an operational risk management process to assess the identified risks in terms of likelihood and impact.										
9. Risk control and mitigation should be a step of an operational risk management process to establish risk control measures for the identified risks.										
10. Risk monitoring should be a step of an operational risk management process to ensure the continuous monitoring and reporting of risks and control measures.										
11. Organisations should appoint employees who are responsible for identified critical functions during a crisis event.										
12. Employees should be trained to understand and perform their functions during a crisis event.										
	A. Your view on importance					B. Current applicability in your organisation				
13. Organisations should ensure a health and safety environment for employees during times of a crisis.										
14. Organisations should develop adequate policies and procedures to ensure the continued operations of business processes during times of a crisis.										
15. Policies and procedures should stipulate effective communication strategies between all stakeholders to ensure the flow of essential business information to ensure continued business operations.										
16. A Business Continuity Management policy should be approved and include a detailed Business Continuity Planning process that deals with a crisis.										
	A. Your view on importance					B. Current applicability in your organisation				
17. A cyber-security policy should include a process to ensure data and information security.										
18. A continuous training communication process should be established to inform all stakeholders on cyber activities or threats.										
19. A data backup facility should be established to protect an organisation from losing critical data due to a disruption caused by a crisis event.										
	A. Your view on importance					B. Current applicability in your organisation				

20. BCM should be developed to ensure business continuity during a crisis.										
21. BCM should include all stakeholders responsible for business continuity during a disruption.										
22. BCM should include a process for dealing with the crisis that could disrupt the business or threaten the safety of employees.										
23. A BCP should be defined to ensure that all stakeholders understand their roles and responsibilities during a crisis.										
24. Training drills should be performed to test the effectiveness of the BCP.										
25. BCM should identify critical functions of an organisation that should remain operational during a crisis.										
26. A BCP should stipulate which functions can be performed remotely during a crisis event.										

Please save the document and return to: Matokelo Motopi

THANK YOU

The records will be kept for five years for audit purposes and will, thereafter, be permanently destroyed by way of being deleted from the hard drives of the computers used to store them. There is no financial compensation or incentive for your participation in the survey.

The research has been reviewed and approved by the UNISA College of Economic and Management Sciences Research Ethics Review Committee, Ethics clearance number: 1709. The primary researcher, Matokelo Nteboheleng Motopi, can be contacted during office hours at 7:30 to 18:30 pm

Annexure B: Email cover page for a questionnaire



PARTICIPANT INFORMATION SHEET

Ethics clearance reference number: 1709

Research permission reference number (if applicable): <date>

Title: OPERATIONAL RISK CONTROL MEASURES for the Lesotho Banking Industry to manage a crisis event: Case study of Covid-19 pandemic

Dear Prospective Participant

My Name is Matokelo Nteboheleng Motopi and I am doing research with Professor Jackie Young a professor in the Department of finance, banking and risk management towards a master's in business management the University of South Africa. We are inviting you to participate in a study entitled Operational risk controls measures for the Lesotho banking industry to manage a crisis event: case study of Covid-19 Pandemic.

This study is expected to collect important information that could confirm the importance of operational risk control measures that a bank should embed to effectively manage potential risks caused by a crisis event and to confirm the status of these control measures in the Lesotho banking industry.

Banking industry is an essential sector that must remain operational during a crisis event; therefore, it is important to identify how banking services should be continued during a crisis event while at the same time mitigating operational risks to the banks. An application letter to conduct the study using your organization as a participant was sent to the organization. The letter indicated that targeted population for this study were all officials, managers and executives within the bank who work directly with operational risk management of the banks. Four Lesotho banks have been identified to participate in this study and the number of participants from each bank will differ depending on the organizational structures.

The questionnaire is divided in two sections. section 1, the participant is required to mark his or her answer with **X** in the space provided and in section 2, the participant is required to answer the questions by indicating with an **X** in the appropriate space provided based on their knowledge and experience. A questionnaire contains closed ended questions in a Likert form, scale from 1 to 5, to no degree - to full degree. It should take approximately 15 minutes to complete the survey.



This survey is voluntary and all information will be regarded as confidential. No names will be linked to any feedback and data will be anonymous. You are, however, under no obligation to complete the survey and you can withdraw from the study before submitting it.

If you choose to participate in this survey, it will take no more than 15 minutes of your time. You will not directly benefit from your participation as an individual, but can add value towards the objective of this research. The questions require participants to indicate the extent to which their organisations currently apply the identified operational risk controls as part of their risk management. Participants may fear that in answering some of the questions especially providing negative feedback, they may expose their weaknesses to competitors or the regulator. However, feedback will not be linked to individual participants; rather the study will just be generic to the entire banking industry.

All information of the research is regarded as confidential. No names will be attached to the data. Data will be password protected and only authorized personnel (The researcher, supervisor and the statistician) will have access. Authorized personnel will sign a confidentiality agreement. Additionally, no personal identification will be required from the participant.

Electronic information will be stored on a password protected computer for 5 years. Future use of the stored data will be subject to further Research Ethics Review and approval if applicable (such as using the data for a purpose unrelated to the initial aim and objectives of the study). Information will be destroyed if necessary. Hard copies will be shredded, and/or electronic copies will be permanently deleted from the hard drive of the computer using a relevant software programme. You will not directly benefit from your participation as an individual or receive any financial incentive for your participation.

This study has received written approval from the Research Ethics Review Committee of the College of Economic Management and science ERC, Finance, Banking and Risk Management, Unisa. A copy of the approval letter is attached with the questionnaire.

If you would like to be informed of the final research findings, please contact Matokelo Motopi at matokelomotopi26@gmail.com , Cell. +266 58042121 and Tel. +266 22232455.

Should you require any further information or want to contact the researcher about any aspect of this study, please contact at matokelomotopi26@gmail.com , Cell +266 58042121 and Tel. +266 22242455.

Should you have concerns about the way in which the research has been conducted, you may contact Youngj@worldonline.ac.za. Contact the research ethics chairperson of the Committee of the College of Economic Management and science ERC, Finance, Banking and Risk



Management Professor Ashley Muteza, contacts 0124294595, muteza@unisa.ac.za if you have any ethical concerns.

Thank you for taking time to read this information sheet and for participating in this study.

Thank you.



Matokelo Nteboheleng Motopi



University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

Annexure C: Consent form



CONSENT TO PARTICIPATE IN THIS STUDY

I, _____ (participant name), confirm that the person asking my consent to take part in this research has told me about the nature, procedure, potential benefits and anticipated inconvenience of participation.

I have read (or had explained to me) and understood the study as explained in the information sheet.

I have had sufficient opportunity to ask questions and am prepared to participate in the study.

I understand that my participation is voluntary and that I am free to withdraw at any time without penalty (if applicable).

I am aware that the findings of this study will be processed into a research report, journal publications and/or conference proceedings, but that my participation will be kept confidential unless otherwise specified.

I agree to the recording of the <insert specific data collection method>.

I have received a signed copy of the informed consent agreement.

Participant Name & Surname..... (please print)

Participant Signature.....Date.....

Researcher's Name & Surname.....(please print)

Researcher's signature.....Date.....



Annexure D: Diagnostic results

1. 1. The survey's purpose is distinct.								
Option	Strongly disagree	Disagree	Neutral	Strongly agree	Agree	Median	Average	Mode
	0%	0%	0%	50%	50%	4.5	4.5	4
2. 2. The questions are relevant to the study's purpose.								
Option	Strongly disagree	Disagree	Neutral	Strongly agree	Agree	Median	Average	
	0%	0%	0%	50%	50%	4.5	4.5	4
3. The survey is inclusive in terms of operational risk controls for banks during a crisis event								
Options	Strongly disagree	Disagree	Neutral	Strongly agree	Agree	Median	Average	Mode
				25%	75%	4	4.25	4
4. The guidelines to complete the survey are distinct								
Options	Strongly disagree	Disagree	Neutral	Strongly agree	Agree	Median	Average	Mode
	0%	0%	0%	50%	50%	4.5	4.5	4
5. The questionnaire is constructed logically.								
Options	Strongly disagree	Disagree	Neutral	Strongly agree	Agree	Median	Average	Mode
	0	0	25%	50%	25%	4.5	4.25	5
6. The assertions are easy to understand.								
Options	Strongly Disagree	Disagree	Neutral	Strongly agree	Agree	Median	Average	Mode
	0	0	0	50%	50%	4.5	4.5	4
7. The survey's magnitude is adequate.								
Options	Strongly Disagree	Disagree	Neutral	Strongly agree	Agree	Median	Average	Mode
				50%	50%	4.5	4.5	4
8. Section A of the survey rates the importance of operational risk control measures that a bank should embed to effectively manage potential risks caused by a crisis event								
Options	Strongly disagree	Disagree	Neutral	Strongly agree	Agree	Median	Average	Mode

	0%	0%	0%	50%	50%	4.5	4.5	4
9. Section B determines the current applicability of the confirmed operational risk control measures in an organisation								
Options	Strongly disagree	disagree	Neutral	Strongly agree	Agree	Median	Average	Mode
	0%	0%	0%	25%	75%	4	4.25	4
10. Do you have any questions you'd want to include in the survey?								
Options					Response			
Yes					0%			
No					100%			
11. Indicate the time taken to complete the survey								
Option	0-5 min	6-10 min	7-15 min	16-20 min	21-25 min			
0%	25%	25%	50%	0%	0%			
12. Additional comments: No additional questions were added however, grammatical errors that were identified were corrected.								

Annexure E: Reliability calculator

Case Processing Summary

		N	%
Cases	Valid	41	100.0
	Excluded	0	.0
	Total	41	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.943	26

Annexure F: Ethical clearance certificate



College of Economic and Management Sciences_ERC

Finance, Risk Management
& Banking

Date: 02/11/2023

Dear: Mrs MATOKELO NTEBOHELENG MOTOPI

Ref #: 1709

Name: Mrs MATOKELO NTEBOHELENG
MOTOPI

Student #: 60018712

**Decision: Ethics Approval from
02/11/2023 to 01/11/2025**

Researcher: Mrs MATOKELO NTEBOHELENG MOTOPI

UNISA

LADYBRAND

60018712@MYLIFE.UNISA.AC.ZA +266 58042121

Supervisor: Professor Jackie Young youngj@worldonline.co.za

OPERATIONAL RISK CONTROL MEASURES for the Lesotho Banking Industry to manage a crisis event:
Case study of
Covid-19 pandemic.

Qualification: MCom in Business Management: Department of
Finance, Risk Management and Banking

Thank you for the application for research ethics clearance by the College of Economic and Management Sciences_ERC Finance, Risk Management & Banking for the above-mentioned research study ethics approval is granted for two years.

The **low-risk application** was **reviewed** by the College of Economic and Management Sciences_ERC Finance, Risk Management & Banking on 31/10/2023 in compliance with the Unisa Policy on Research Ethics and the Standard Operating Procedure on Research Ethics Risk Assessment.

The proposed research may now commence with the provisions that:

1. The researcher(s) will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.
2. Any adverse circumstance arising in the undertaking of the research project that is relevant to the ethicality of the study should be communicated in writing to the College of Economic and Management Sciences_ERC Finance, Risk Management & Banking .
3. The researcher(s) will conduct the study according to the methods and procedures set out in the approved application.
4. Any changes that can affect the study-related risks for the research participants, particularly in terms of assurances made with regards to the protection of participants' privacy and the confidentiality of the data, should be reported to the Committee in writing, accompanied by a progress report.

5. The researcher will ensure that the research project adheres to any applicable national legislation, professional codes of conduct, institutional guidelines and scientific standards relevant to the specific field of study. Adherence to the following South African legislation is important, if applicable: Protection of Personal Information Act, no 4 of 2013; Children's act no 38 of 2005 and the National Health Act, no 61 of 2003.

6. Only de-identified research data may be used for secondary research purposes in future on condition that the research objectives are similar to those of the original research. Secondary use of identifiable human research data requires additional ethics clearance.

7. No field work activities may continue after the expiry date 01/11/2025. Submission of a completed research ethics progress report will constitute an application for renewal, for Ethics Research Committee approval.

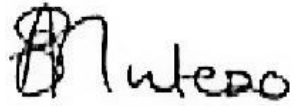
Additional Conditions

1. Disclosure of data to third parties is prohibited without explicit consent from Unisa.
2. De-identified data must be safely stored on password protected PCs.
3. Care should be taken by the researcher when publishing the results to protect the confidentiality and privacy of the university.
4. Adherence to the National Statement on Ethical Research and Publication practices, principle 7 referring to social awareness, must be ensured: "Researchers and institutions must be sensitive to the potential impact of their research on society, marginal groups or individuals, and must consider these when weighing the benefits of the research against any harmful effects, with a view to minimising or avoiding the latter where possible." Unisa will not be liable for any failure to comply with this principle.

Note

The reference number 1709 should be clearly indicated on all forms of communication with the intended research participants, as well as with the committee.

Kind regards,

A handwritten signature in black ink, appearing to read 'A Mutezo'.

Prof A Mutezo

Chair of College of Economic and Management Sciences_ERC
Finance, Risk Management & Banking E-mail: Muteza@unisa.ac.za

A handwritten signature in black ink, appearing to read 'MT Mogale'.

Prof MT Mogale

Executive Dean / By delegation from the Executive Dean of College of Economic and
Management Sciences_ERC Finance, Risk Management & Banking
E-mail: mogalmt@unisa.ac.za

Annexure G: Gate keeper approvals



Mafike House, Kingsway Road
Private Bag A121, Maseru 100
Kingdom of Lesotho
Tel : (+266) 2231 7842
Fax: (+266) 2231 7832
Website : www.lpb.co.ls

Ms. M. Motopi
C/O Central Bank of Lesotho
Maseru

Dear 'Matokelo Motopi,

RE: PERMISSION TO CONDUCT YOUR RESEARCH AT LESOTHO POSTBANK

This letter serves to inform you that your request to conduct a research on topic: "Operational Risk Control Measures for the Lesotho Banking Industry During a Pandemic: A case study of Covid-19", at Lesotho PostBank has been granted with following conditions:

- The research should not interrupt any business activities.
- The findings will be shared with the Bank.
- You will adhere to the stipulations of the signed NDA.
- Anonymity and confidentiality will be observed.
- Participation of employees is voluntary.

The Bank will however do everything in its powers to ensure that this exercise becomes a success. Wish you all the best in your studies.

Yours sincerely

A handwritten signature in black ink, appearing to read "Molloa Molloa", is written over a horizontal line.

Molloa Molloa
Chief People and Culture

Board of Directors: Mrs M. Matela – Mphahla (Chairperson), Mr. R. Mathule (Non – Executive Director), Mrs. M. Mathaleng (Non-Executive Director), Mr. L. Mokete (Non-Executive Director), Mr. M. Leqhae (Managing Director), Mr. M. Mahoana (Executive Director), Mrs. M. Morake (Executive Director), Mr. R. Makara (Corporate Secretary)

UNISA



university
of south africa

GATEKEEPER RESEARCH PERMISSION APPLICATION FORM

A. GATEKEEPER CONTACT INFORMATION

Name of organisation/company/stakeholder/community leader - referred to as the 'gatekeeper:

NEDBANK LESOTHO

Contact person (name and surname):

Mr. NKÄU MÄTETE

Designation/position within company/organisation/community:

MANAGING DIRECTOR

Email:

nmatete@nedbank. co . ls

Contact number:

+266 58850029

2

B. APPLICANT INFORMATION

FROM:

Name and surname of applicant/student/researcher:

MATOKELO NTEBOHELENG MOTOPI

Degree registered for or research for non-degree purposes:

MASTERS IN BUSINESS MANAGEMENT (FINANCE, BANKING A-ND RISK MANAGEMENT)

Department and College:

UNISA: ECONOMIC A-ND MANAGEMENT SCIENCE

Email:

60018712@mylife.unisa.ac.za

Contact number:

+266-58042121 and 22232455

Address:

CENTRAL BANK OF LESOTHO

Details of supervisor (if applicable):

PROF. YOUNG JACKIE

Email of supervisor (if applicable):

Youngj@worldonline.co.za

3

Supervisory position, e.g. lecturer (senior lecturer/professor, etc.):

PROFESSOR

Supervisor's Department:

DEPARTMENT OF FINANCE, BANKING AND RISK MANAGEMENT

Funding Body (if applicable):

CENTRAL BANK OF LESOTHO

Reason for funding (if applicable):

EMPLOYEE SKILL EMPOWERMENT

c. REQUEST FOR SUPPORT/ ACCESS TO DATA/INFORMATION/ PARTICIPANTS

I/We are requesting your assistance in a study entitled:

OPERATIONAL RISK CONTROL MEASURES FOR THE LESOTHO BANKING INDUSTRY DURING

Overview of study: (100-200 words)

- What, how and why of the study
- Objectives, time and resources used/required
- Deadline/timelines for the project - possibility of follow up interviews? If further information will be required

Banks are critical to any economy and play an important role in ensuring financial stability- If no profits are made, loans and other financial services cannot be offered, depriving the economy of the credit it requires. Lesotho's economy is recognised for its poor economic growth and significant unemployment, notwithstanding recent improvements in bank financial performance (Central Bank of Lesotho supervisory report, 2020). The COVID-19 pandemic, on the other hand, occurred in 2020, affecting the country' s economy and potentially creating an economic crisis. Strict procedures, such as country lockdowns, were put in place to reduce the spread of the pandemic. Nonetheless, being a critical service, the banking industry had to remain operational during the shutdown. Only the bank's critical activities were carried out on-site, while the rest were carried out remotely. As a result,' the study proposes to analyse how COVID-19 influenced the banking industry and identify potential operational risk controls that banks could adopt to prepare for future pandemics. UNISA requires a researcher to request permission from organisations to participate in the study as part of an ethical review.

The signed consent of the participants will thus be used to apply for ETHICAL CLEARANCE to allow the researcher to gather data. The questionnaire (survey) must be launched be March 31, 2023.

4

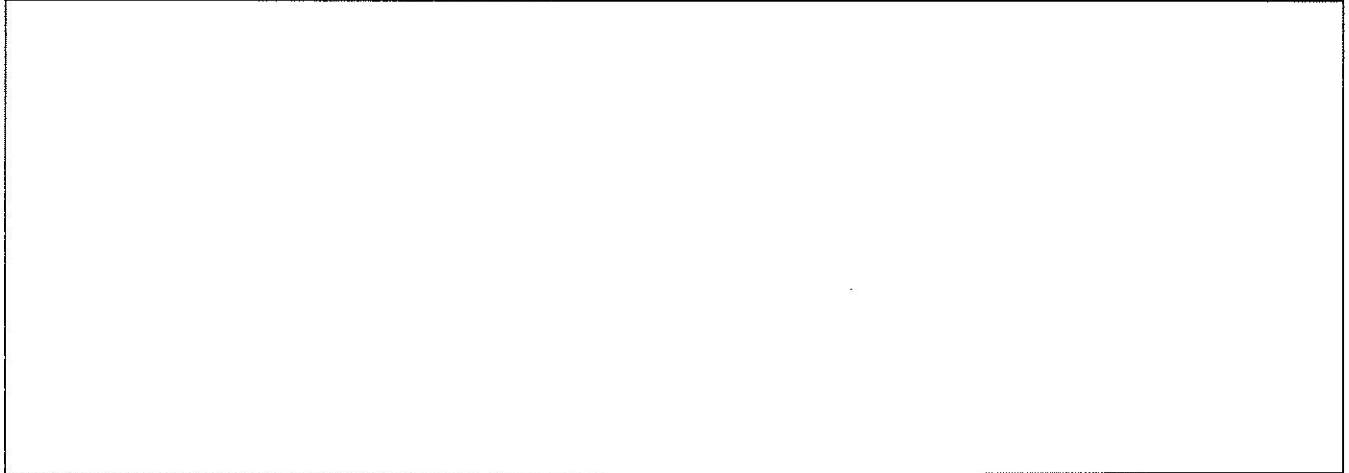
My/our request is/are for: (Tick appropriate options and/or add additional information.)

- Permission and/or support to conduct a study about or within the organisation/company/stakeholder group/community
- Access to possible participants and assistance for recruitment and identification purposes
- Assistance in the recruitment process of possible participants via internal communication
- Permission to distribute questionnaire/survey/research information to potential participants
- Access to organisational data - not in the public domain
- Other (specify below):

Provide a full description of the intended research sample. Motivate why the data must be gathered from the specific stakeholder group/organisation/company/community.

The intended sample will include managers and senior managers who work directly with the bank's operational risk management.

5



Explain how the participant identification and recruitment process of your research adhere to the Protection of Personal Information Act 4 of 2013.

The researcher will seek the participants' approval to conduct the study and responses will be fully anonymous

Provide a description of the data collection tools (e.g. interview, questionnaire, questions).

questionnaire will be used to collect data. It will consist of 30 questions including the Biography questions. The questions will be close ended in a Likert scale form and it should take up to 15 min to complete the survey.

6

Provide a description of the data gathering process that will be followed. (What will be expected of the research participants and exactly how will the data be collected?)

The participant will be required to indicate with a tick, his department and area of focus within the organisation, years of experience in risk management and years of experience in current position. Question 5 consists of 26 questions divided in two sections. The questions are in a 5 Likert scale from To no degree to, To full degree. In Section A, the participants will have to rate the IMPORTANCE of the operational risk control measure which a bank should embed to effectively manage potential risks caused by disastrous incidents. Section B on the other hand the participants will rate the extent they agree that the operational risk control measures are CURRENTLY applicable as part of risk management in their organisation

Indicate who will have access to the raw data and in what formats?

The questionnaire will be shared as a link and only the researcher, and a supervisor and a statistician will have access to the raw data.

Provide a full description of the perceived and actual risks of the study to participants and the organisation/company/stakeholder group/community. (Keeping national disasters in mind.)

Competitors may learn about the participant s weaknesses.

Describe the potential benefits of the study to the organisation/company/stakeholder group/community.

Based on the results of the study, the participant will be able to determine the level of operational risk management for banks in the country and learn from the gap analysis obtained by the researcher between the importance and the current applicability of the operational risk control measures, which the researcher will indicate in the recommendation section of the study.

How will risks be mitigated and managed? (Keeping national disasters and relevant protocol in mind.)

Despite the fact that participation will be completely anonymous, the research will not be done on individual bank; rather, it will be an analysis of the country's overall banking sector.

Explain the extent and processes to which confidentiality of information will be maintained by the researcher.

The researcher will ensure that participation in this study is voluntary, participants will not be deceived and will be fully anonymous. The responses from the questionnaire will be password protected to avoid any unauthorised access to the data.

8

List the expected deliverables of the study. (For example, a research report, journal articles and/or conference proceedings. Also indicate how privacy will be protected in any publication of the information.)

Research report and a journal article.

How will the organisation/company/stakeholder group/community be informed of the results or outcomes? (If applicable.)

A copy of the research report and the journal article will be availed to the participant through direct channels .

Attach a copy of the research instrument (questionnaire interview schedule/focus Zoup questions) to your email and mark as Annexure A

c. OFFICIAL USE ONLY - TO BE COMPLETED BY COMPANY/ORGANISATION/COMMUNITY

Decision:

Permission granted.

Permission with conditions is granted.

[2 No permission could be granted at this time.

Special Conditions (if any - Expectations of the outcomes of the study must be stated. For example: Will feedback/a report be required before submission of the publication?):

Permission granted with conditions to treat all information with confidentiality in line with data privacy Act and other CBL regulations. The Researcher is required to preserve personally identifiable information confidential in line with the laws governing Nedbank Lesotho.

The following person and/or department/and or committee has been appointed to assist the researcher in the data collection process (if applicable):

Rarnoj apoho Moshoeshoe

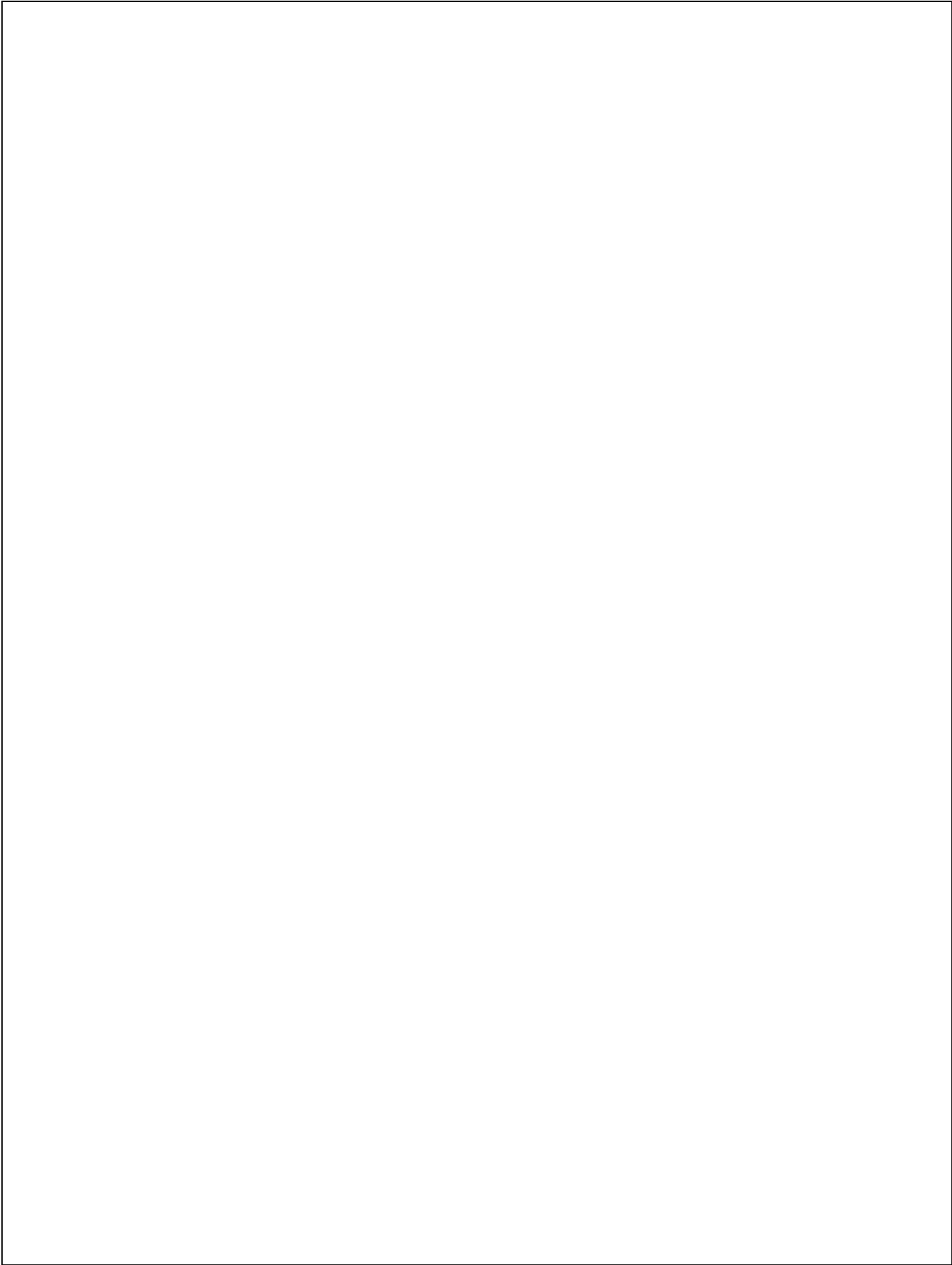
By signing this form, you are indicating that you have read the description of the study, have the legal and delegated authority to grant permission for the study on behalf of the company or organisation and stakeholder/ community and that the company/organisation/stakeholder/community in principle agrees to the terms as described in the short questionnaire that follows:

1. I/We have reviewed the application form and received a copy of it. The purpose and nature of this study are clear, and all questions and issues of concern have been answered to satisfaction.

Yes

2. I/We (name of the person responsible and/or name of company/organisation/stakeholder/community)

Ramojapoho Moshoeshoe



agree to support this study and hereby grant permission for the data generated from this research to be used in the researcher's publications on this topic.

Signature



Name and surname of the person with delegated authority to grant permission on behalf of the company/organisation/stakeholder/community

Ramojapoho Moshoeshoe

Designation/Position

Chief Risk Officer

Email:

rmoshoeshoe@nedbank.co.ls

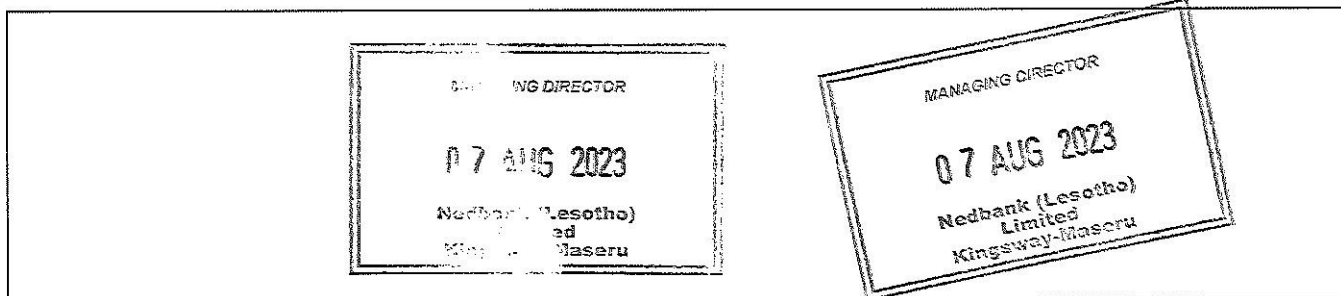
Contact number:

+266 62100903

Date:

07/08/2023

Official stamp (if available):





GATEKEEPER RESEARCH PERMISSION
APPLICATION FORM

A. GATEKEEPER CONTACT INFORMATION

TO:

Name of organisation/company/stakeholder/community leader - referred to as the 'gatekeeper':

CENTRAL BANK OF LESOTHO

Contact person (name and surname):

Mrs Mateboho Morojele

Designation/position within company/organisation/community:

Director Human Resource

Email:

mmorojele@centralbank.org.ls

Contact number:

+266 222 32 004

B. APPLICANT INFORMATION

FROM:

Name and surname of applicant/student/researcher:

MATOKELO NTEBOHELENG MOTOPI

Degree registered for or research for non-degree purposes:

MASTERS IN BUSINESS MANAGEMENT (FINANCE, BANKING AND RISK MANAGEMENT)

Department and College:

UNISA: ECONOMIC AND MANAGEMENT SCIENCE

Email:

60018712@mylife.unisa.ac.za

Contact number.

+266-58042121 and 22232455

Address:

CENTRAL BANK OF LESOTHO

Details of supervisor (if applicable):

PROF. YOUNG JACKIE

Email of supervisor (if applicable):

Youngj@worldonline.co.za

Supervisors position, e.g. lecturer/senior lecturer/professor, etc.:

PROFESSOR

Supervisor's Department:

DEPARTMENT OF FINANCE, BANKING AND RISK MANAGEMENT

Funding Body (if applicable):

CENTRAL BANK OF LESOTHO

Reason for funding (if applicable):

EMPLOYEE SKILL EMPOWERMENT

c. REQUEST FOR SUPPORT/ ACCESS TO DATA/INFORMATION/ PARTICIPANTS

I/We are requesting your assistance in a study entitled:

OPERATIONAL RISK CONTROL MEASURES FOR THE LESOTHO BANKING INDUSTRY TO MANP.

Overview of study: (100-200 words)

- What, how and why of the study
- Objectives, time and resources used/required
- Deadline/timelines for the project - possibility of follow up interviews? If further information will be required

Banks are critical to any economy and play an important role in ensuring financial stability. If no profits are made, loans and other financial services cannot be offered, depriving the economy of the credit it requires. Lesotho's economy is recognised for its poor economic growth and significant unemployment, notwithstanding recent improvements in bank financial performance (Central Bank of Lesotho supervisory report, 2020) The COVID—19 pandemic, on the other hand, occurred in 2020, affecting the country's economy and potentially creating an economic crisis. Strict procedures, such as country lockdowns, were put in place to reduce the spread of the pandemic. Nonetheless, being a critical service, the banking industry had to remain operational during the shutdown. Only the bank's critical activities were carried out on—site, while the rest were carried out remotely. As a result, the study proposes to analyse how COVID-19 influenced the banking industry and identify potential operational risk controls that banks could adopt to prepare for future pandemics.

UNISA requires a researcher to request permission from organisations to participate in the study as part of an ethical review.

The signed consent of the participants will thus be used to apply for ETHICAL CLEARANCE to allow the research to gather data. The questionnaire (survey) must be Launched by March 31, 2023.

My/our request is/are for: (Tick appropriate options and/or add additional information.)

C) Permission and/or support to conduct a study about or within the organisation/company/stakeholder group/community

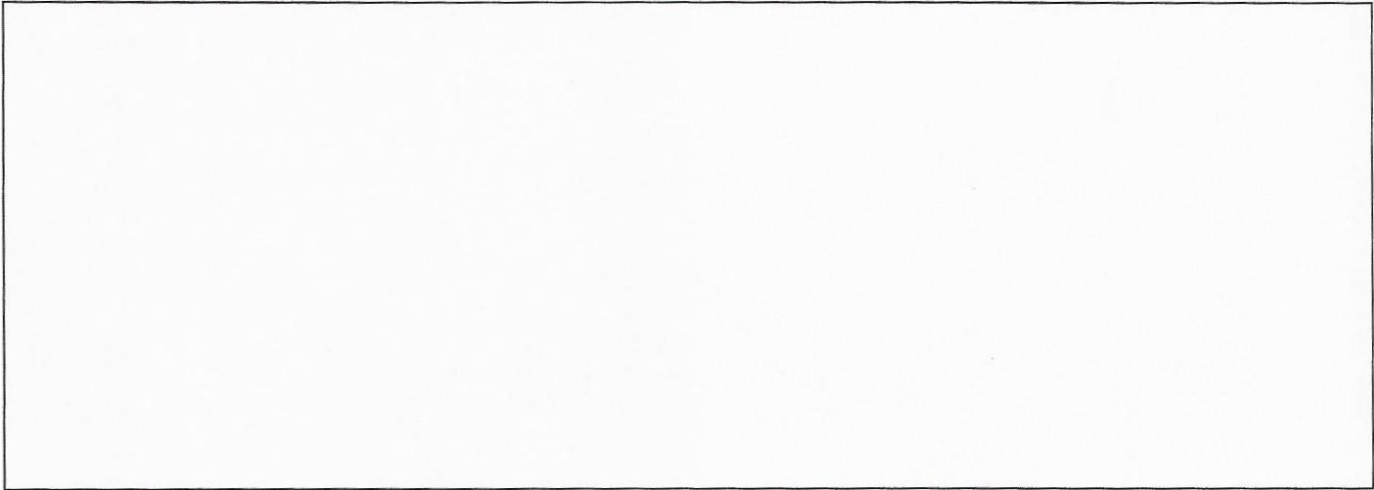
C] Access to possible participants and assistance for recruitment and identification purposes

C] Assistance in the recruitment process of possible participants via internal communication

Permission to distribute questionnaire/survey/research information to potential participants C] Access to organisational data — not in the public domain C] Other (specify below):

Provide a full description of the intended research sample. Motivate why the data must be gathered from the specific stakeholder group/organisation/company/community.

The intended sample will include managers and senior managers who work directly with the bank's operational risk management.



Explain how the participant identification and recruitment process of your research adhere to the Protection of Personal Information Act 4 of 2013.

The researcher will seek the participants' approval to conduct the study and responses will be fully anonymous

Provide a description of the data collection tools (e.g. interview, questionnaire, questions).

questionnaire will be used to collect data. It will consist of 30 questions including the Biography questions. The questions will be close ended in a Likert scale form and it should take up to 15 min to complete the survey.

Provide a description of the data gathering process that will be followed. (What will be expected of the research participants and exactly how will the data be collected?)

The participant will be required to indicate with a tick, his department and area of focus within the organisation, years of experience in risk management and years of experience in current position. Question 5 consists of 26 questions divided in two sections. The questions are in a 5 Likert scale from To no degree to, To full degree. In Section A, the participants will have to rate the IMPORTANCE of the operational risk control measure which a bank should embed to effectively manage potential risks caused by disastrous incidents. Section B on the other hand the participants will rate the extend the agree that the operational risk control measures are CURRENTLY applicable as part of risk management in their organisation.

Indicate who will have access to the raw data and in what formats?

questionnaire will be shared as a link and only the researcher, statistician and supervisor and will have access to the raw data.

Provide a full description of the perceived and actual risks of the study to participants and the organisation/company/stakeholder group/community. (Keeping national disasters in mind.)

Competitors may learn about the participant 's weaknesses.

Describe the potential benefits of the study to the organisation/company/stakeholder group/community.

Based on the results of the study, the participant will be able to determine the level of operational risk management for banks in the country and learn from the gap analysis obtained by the researcher between the importance and the current applicability of the operational risk control measures, which the researcher will indicate in the recommendation section of the study.

How will risks be mitigated and managed? (Keeping national disasters and relevant protocol in mind.)

Even though participation will be completely anonymous, the research will not be done on individual bank; rather, it will be an analysis of the country's overall banking sector. Explain the extent and processes to which confidentiality of information will be maintained by the researcher.

The researcher will ensure that participation in this study is voluntary, participants will not be deceived and will be fully anonymous. The responses from the questionnaire will be password protected to avoid any unauthorised access to the data.

List the expected deliverables of the study. (For example, a research report, journal articles and/or conference proceedings. Also indicate how privacy will be protected in any publication of the information.)

Research report and a journal article.

How will the organisation/company/stakeholder group/community be informed of the results or outcomes? (If applicable.)

A copy of the research report and the journal article will be availed to the participants through direct channels.

Attach a copy of the research instrument (questionnaire/interview schedule/focus group questions) to your email and mark as Annexure A

c. OFFICIAL USE ONLY - TO BE COMPLETED BY
COMPANY/ORGANISATION/COMMUNITY

Decision:

Permission granted.

T] Permission with conditions is granted.

C] No permission could be granted at this time.

Special Conditions (if any - Expectations of the outcomes of the study must be stated. For example: Will feedback/a report be required before submission of the publication?):

The following person and/or department/and or committee has been appointed to assist the researcher in the data collection process (if applicable):

Mateboho Morojele (Mrs.), Director of Human Resources

By signing this form, you are indicating that you have read the description of the study, have the legal and delegated

authority to grant permission for the study on behalf of the company/organisation/stakeholder/community

and that the company/organisation/stakeholder/community in principle agrees to the terms as described in the short questionnaire that follows:

1. I/We have reviewed the application form and received a copy of it. The purpose and nature of this study are clear, and all questions and issues of concern have been answered to satisfaction. a Yes

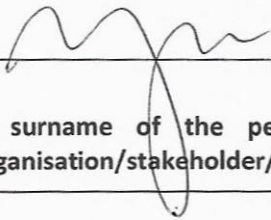
2. I/We (name of the person responsible and/or name of company/organisation/stakeholder/community)

'Mateboho Morojele

agree to support this study and hereby grant permission for the data generated from this research to be used in the researcher's publications on this topic.

Yes

Signature



Name and surname of the person with delegated authority to grant permission on behalf of the company/organisation/stakeholder/community

'Mateboho Morojele

Designation/Position

Director of Human Resources

Email:

mmorojele@centralbank.org.ls

Contact number:

+266 222 32 004

Date:

16 August 2023

Official stamp (if available):

CENTRAL BANK OF
LESOTHO

2023 -08- 16

HUMAN
RESOURCES

P.o. BOX • MASERU

Annexure H: Checklist

Number	Risk control measure	Checkmark the appropriate column	
		Yes	No
1	Operational risk should be clearly defined and understood by all employees of the bank.		
2	An operational risk management framework should be embedded to serve as a platform to guide effective operational risk management.		
3	A risk culture should ensure the embedding of norms, attitudes and behaviours of employees relating to risk controls.		
4	A risk management strategy should be aligned with the business strategy to ensure that the objectives are within the set parameters of the risk appetite.		
5	A governance structure should be embedded to confirm the roles and responsibilities of role-players in risk management.		
6	A risk management process should be formalised and embedded in the organisation.		
7	Risk identification should be a step of an operational risk management process to identify the inherent risk exposures.		
8	Risk evaluation should be a step of an operational risk management process to assess the identified risks in terms of likelihood and impact.		

9	Risk control and mitigation should be a step of an operational risk management process to establish risk control measures for the identified risks.		
10	Risk monitoring should be a step of an operational risk management process to ensure the continuous monitoring and reporting of risks and control measures.		
11	Organisations should appoint employees who are responsible for identified critical functions during a crisis event.		
12	Employees should be trained to understand and perform their functions during a crisis event.		
13	Organisations should ensure a health and safety environment for employees during times of a crisis.		
14	Organisations should develop adequate policies and procedures to ensure the continued operations of business processes during times of a crisis.		
15	Policies and procedures should stipulate effective communication strategies between all stakeholders to ensure the flow of essential business information to ensure continued business operations.		
16	A Business Continuity Management policy should be approved and include a detailed Business Continuity Planning process that deals with a crisis.		
17	A data backup facility should be established to protect an organisation from losing critical data due to a disruption caused by a crisis event.		

18	A continuous training communication process should be established to inform all stakeholders on cyber activities or threats.		
19	A data backup facility should be established to protect an organisation from losing critical data due to a disruption caused by a crisis event.		
20	BCM should be developed to ensure business continuity during a crisis.		
21	BCM should include all stakeholders responsible for business continuity during a disruption.		
22	BCM should include a process for dealing with the crisis that could disrupt the business or threaten the safety of employees.		
23	A BCP should be defined to ensure that all stakeholders understand their roles and responsibilities during a crisis.		
24	Training drills should be performed to test the effectiveness of the BCP.		
25	BCM should identify critical functions of an organisation that should remain operational during a crisis.		
26	A BCP should stipulate which functions can be performed remotely during a crisis event.		

Annexure I: Confidentiality agreement statistician



UNISA RESEARCH ETHICS 3rd Party Confidentiality Agreement (Transcriber, Co-coder, Statistician and/or Fieldworkers)

A. INSTRUCTIONS

Please read through the entirety of this form carefully before signing.

After completing the required fields, please sign the form. After this form has been signed by the transcriber, co-coder, statistician or fieldworker, it should be given to the principal researcher for submission to the relevant UNISA Research Ethics Committee.

The transcriber, co-coder, statistician and/or fieldworker should keep a copy of the *Confidentiality Agreement* for their records.

B. CONFIDENTIALITY OF A RESEARCH STUDY

Confidentiality is the treatment and maintenance of information that an individual has disclosed in a relationship of trust and with the expectation that it will not be divulged to others in ways that are inconsistent with the understanding of the original disclosure (the informed consent documentation) without permission. Confidential information relating to human participants in a research study may include, but is not limited to the personal information listed below:

- a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
- b) information relating to the education or the medical, financial, criminal or employment history of the person;

- c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other assignment to the person;
- d) the biometric information of the person;
- e) the personal opinions, views or preferences of the person;
- f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- g) the views or opinions of another individual about the person; and
- h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

As a third party you will have access to research information (e.g. audio or video recordings, DVDs/CDs, transcripts, data, etc.) that include confidential information. Participants have revealed information to the researcher(s) since they have been assured by the researcher(s) that every effort will be made to maintain their privacy throughout the study. That is why it is of the utmost importance to maintain confidentiality when conducting your duties as a transcriber, statistician, co-coder and/or fieldworker during the research study. *Below is a list of expectations you will be required to adhere to in your role as a third party in this study. Review these expectations carefully before signing this form.*

C. THIRD PARTY EXPECTATIONS

To maintain confidentiality, I agree to:

1. Keep all research information that I collect or that is shared with me confidential by not discussing or sharing this information verbally or in any format with anyone other than the principal researcher of this study;
2. Ensure the security of research information (e.g. audio or video recordings, DVDs/CDs, transcripts, data, etc.) while it is in my possession. This includes:

- Keeping all data and/or transcript documents and digitised interviews on a password protected computer with password-protected files;
- Closing any programmes and documents when temporarily away from the computer;
- Keeping any printed transcripts or data in a secure location such as a locked file cabinet;
- Permanently deleting any digital communication containing the data.

3. Not make copies of research information (e.g. audio or video recordings, DVDs/CDs, transcripts, data, etc.) unless specifically instructed to do so by the principal researcher;

4. Give all research information (e.g. audio or video recordings, DVDs/CDs, transcripts, data, etc.) and research participant information, back to the principal researcher upon completion of my duties as a transcriber;

5. After discussing it with the principal researcher, erase or destroy all research information (e.g. audio or video recordings, DVDs/CDs, transcripts, data, etc.) that cannot be returned to the principal researcher upon completion of my duties in this study.

Name of 3rd party involved in research activities:

Research activity responsible for (transcribing interviews, co-coding of data, statistical analysis, collecting data, etc.):

Title of Research Study:

Name of Principal Researcher:

By signing this form, I acknowledge that I have reviewed, understand, and agree to adhere to the expectations described above. I agree to maintain confidentiality while performing my duties as acquired by the principal researcher. I recognise that failure to comply with these expectations may result in legal action.



22/08/2023

Signature of 3rd party

Date

Sejehla Khobotlo

Print Name

Annexure J: Descriptive analysis

Biographical information of the participants

Biographic Information	Response Target per Department	Actual Response per Department	%
Department			
Business Management	15	7	17.1
Financial Management	6	2	4.9
Risk Management	24	11	26.8
Internal Audit	12	8	19.5
Compliance Management	6	3	7.3
Other	15	10	24.4
Focus area			
Business/ Operations Management		10	24.4
Internal Audit		6	14.6
Risk Management		7	17.1
Compliance Management		7	17.1
Financial Management		4	9.8
Other		7	17.1
Years of experience in risk management			
<1		2	4.9
3-<5		11	26.8
5-<10		11	26.8
>=10		17	41.5
Years of experience with your organisation			
3-<5		3	7.3
5-<10		22	53.7
>=10		16	39.0

Figure 5.1: Definition of operational risk management

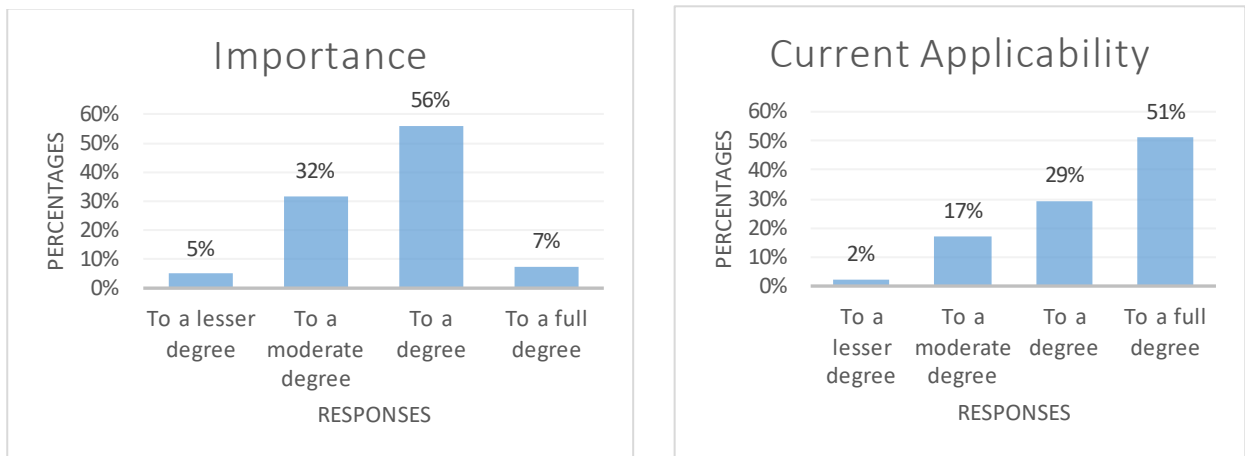


Figure 5.2: Operational risk management framework

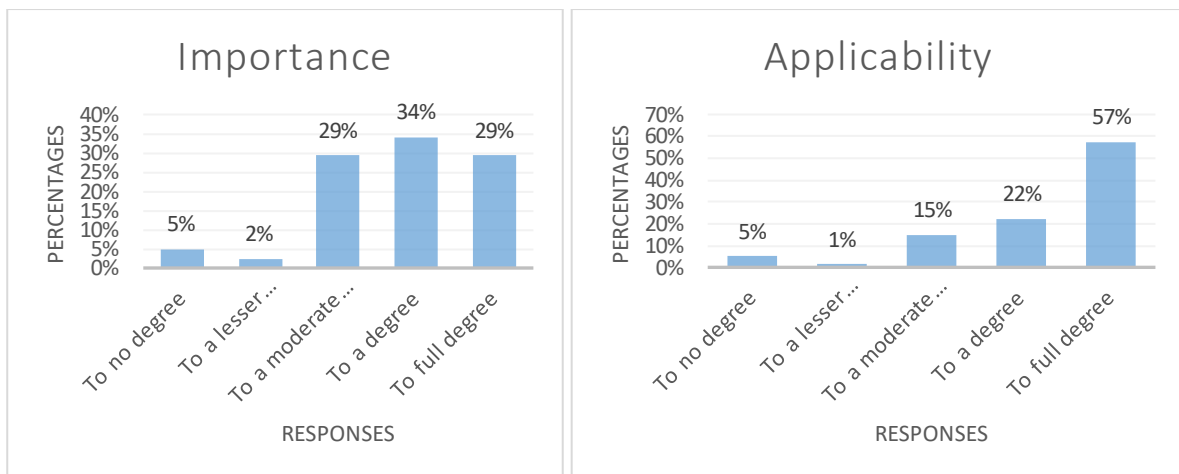


Figure 5.3: Risk culture

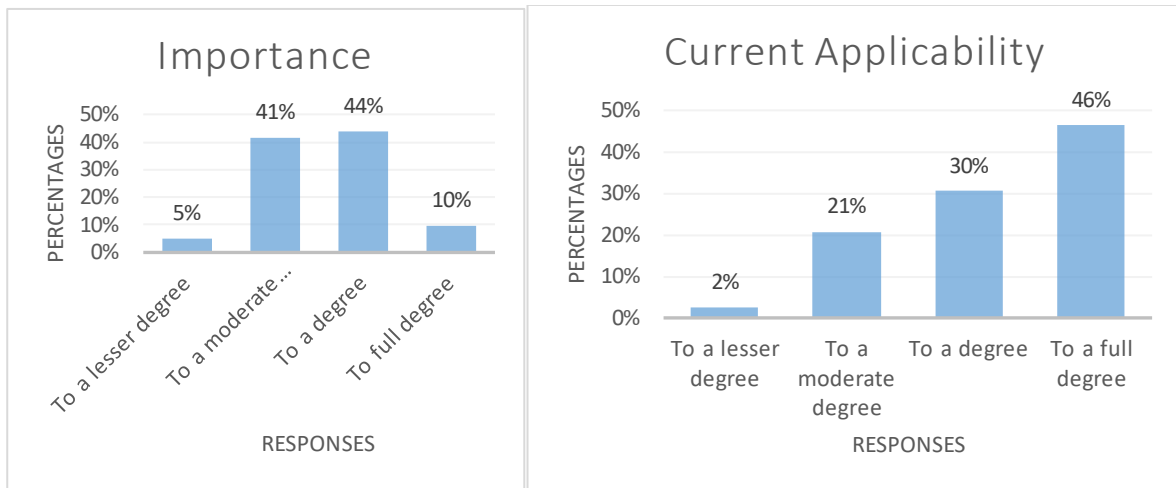


Figure 5.4: Risk management strategy

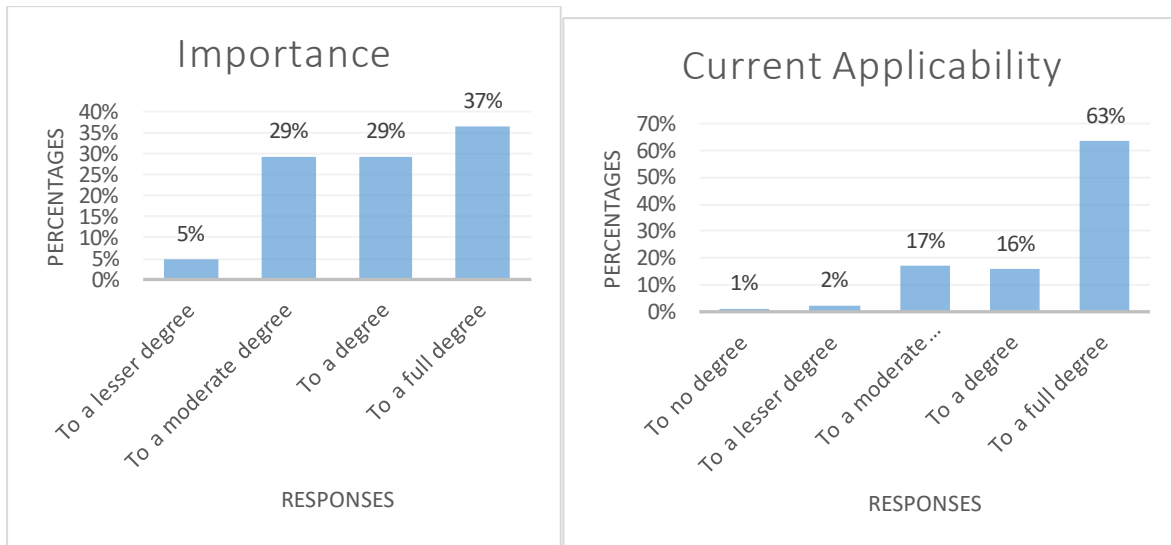


Figure 5.5: Governance structure

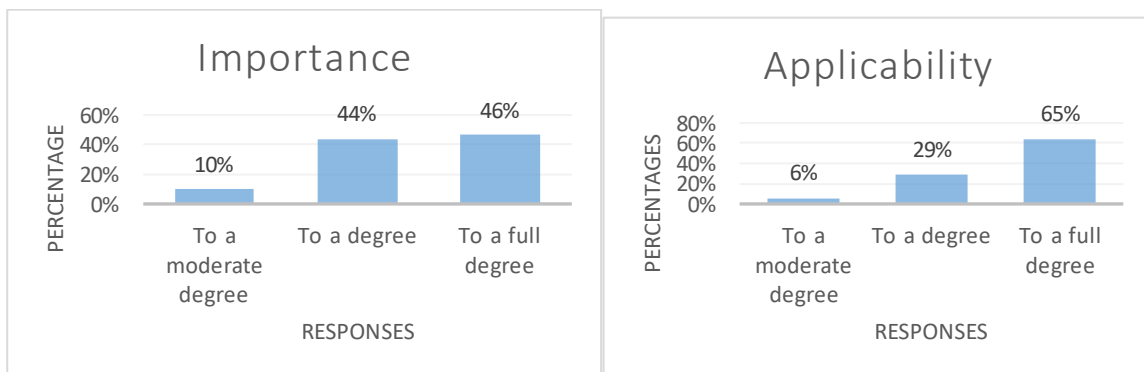


Figure 5.6: Risk management process

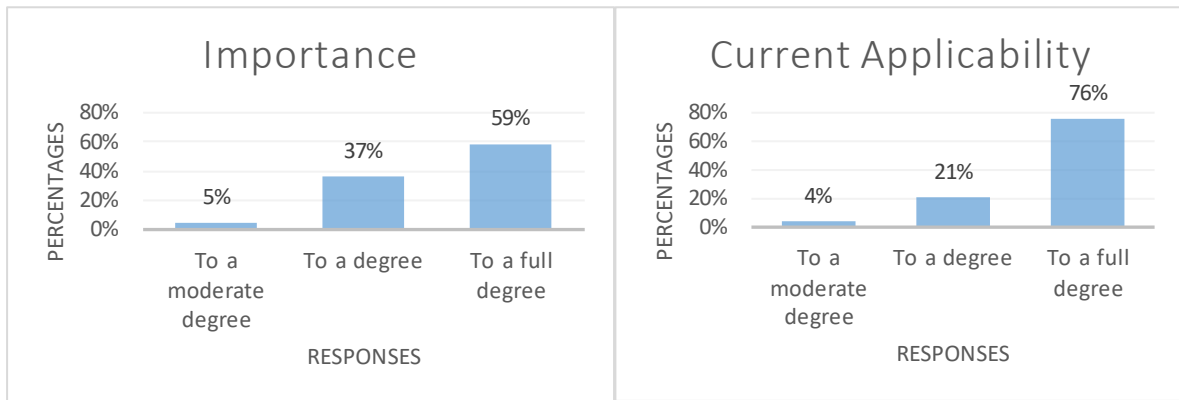


Figure 5.7: Risk identification

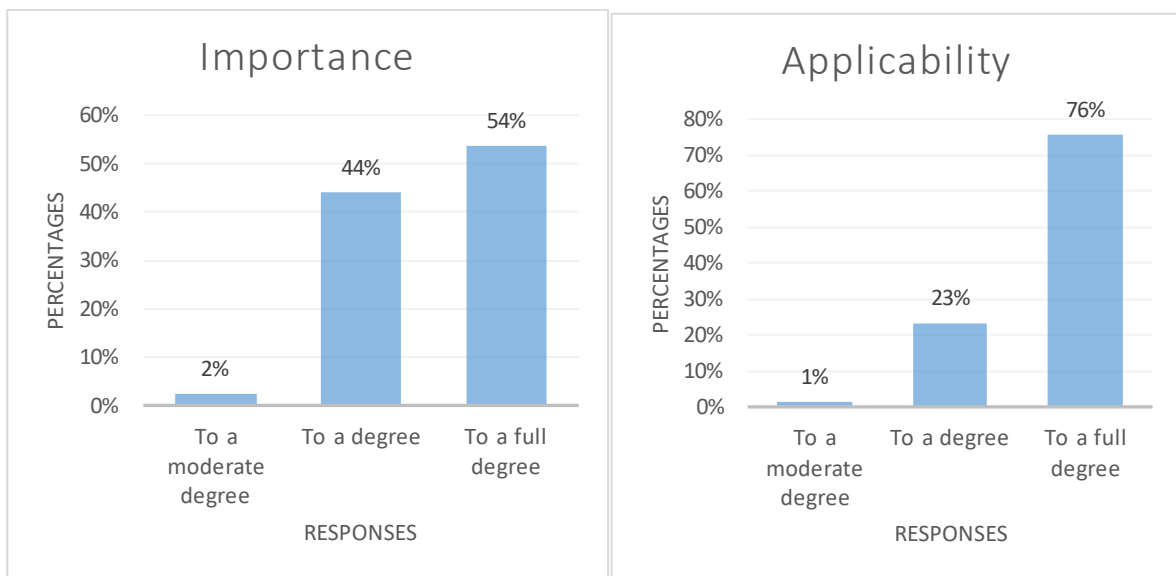
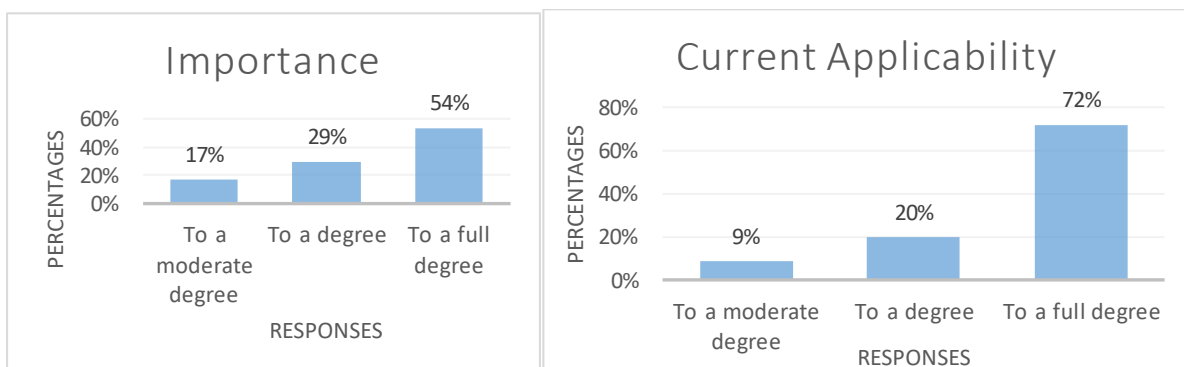


Figure 5.9 Risk control and mitigation



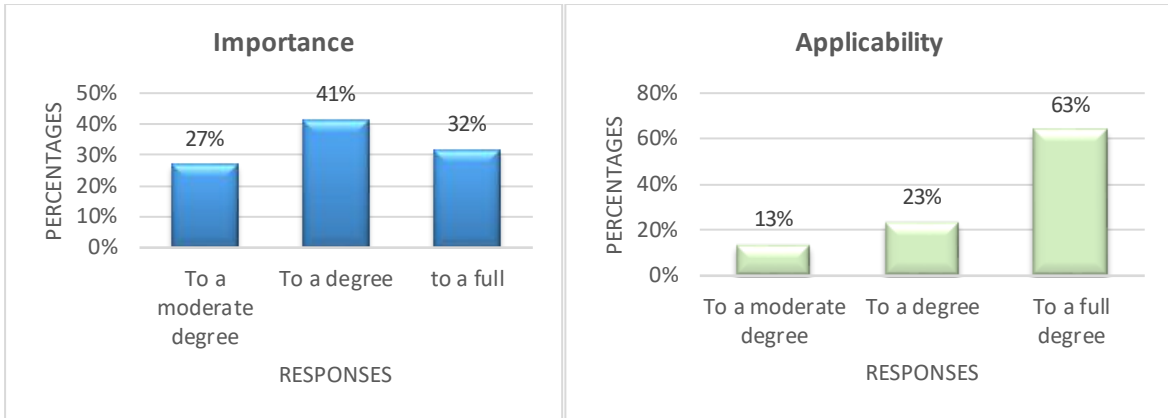


Figure 5.11: Appointing employees for critical functions

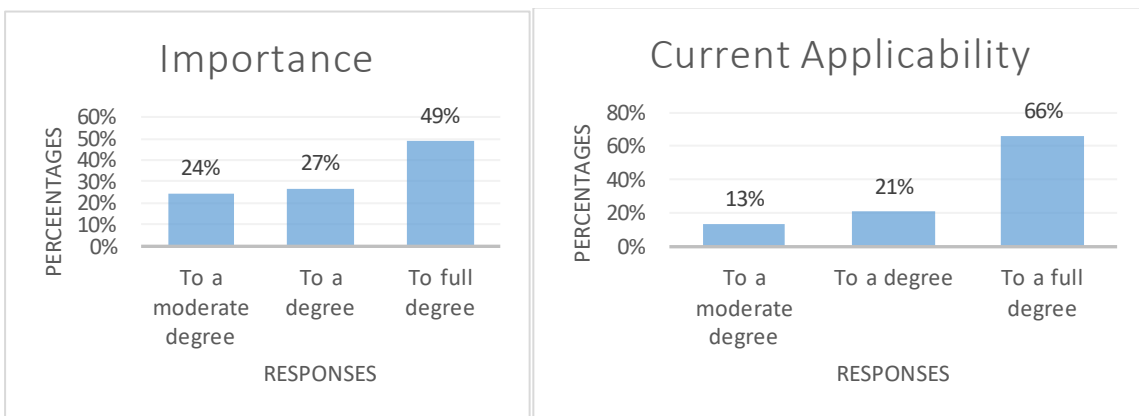


Figure 5.12: Training of employees

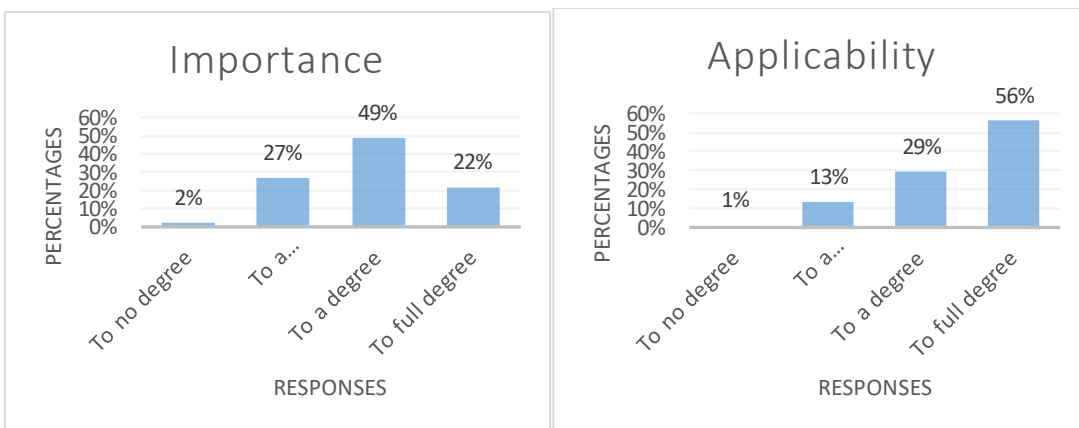


Figure 5.13: Health and safety environment

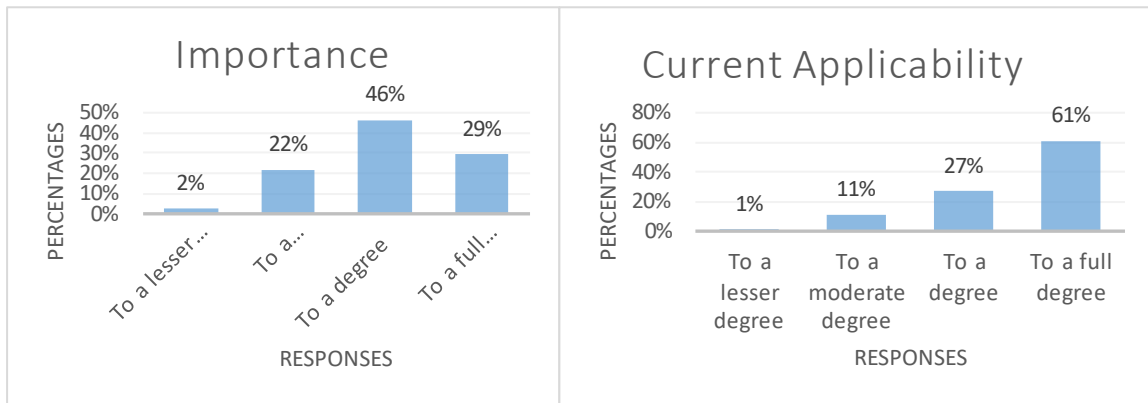


Figure 5.14: Policies and procedures

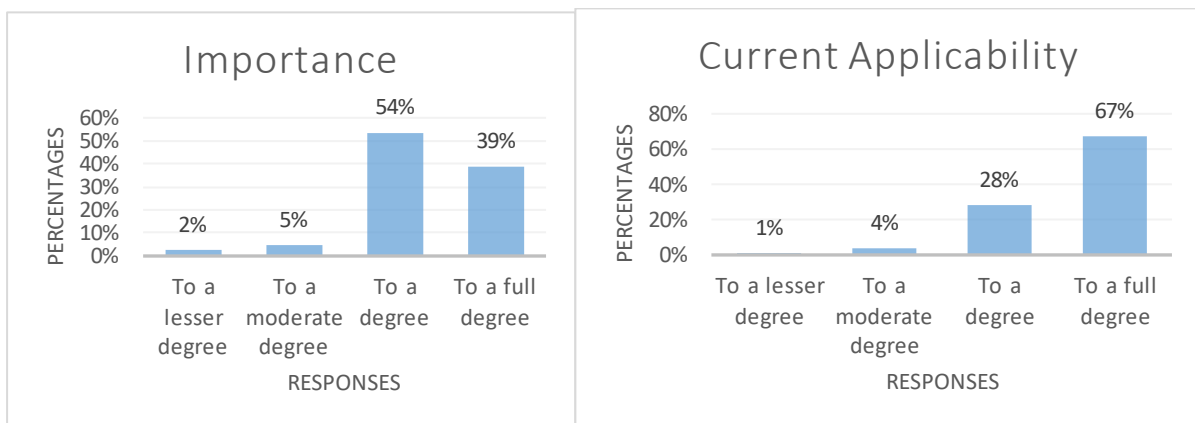
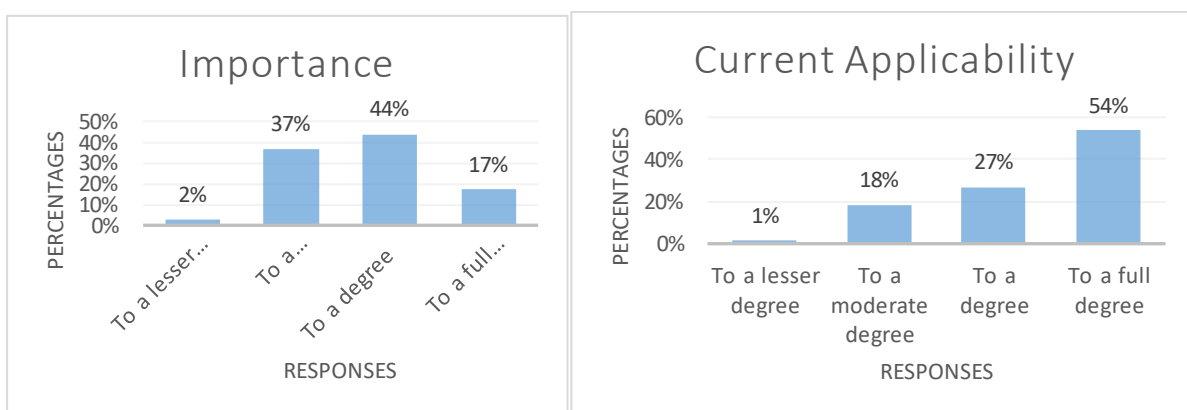


Figure 5.15: Communication strategies to be used during a crisis event



Source: Author's own analysis

Figure 5.16: Business continuity management policy

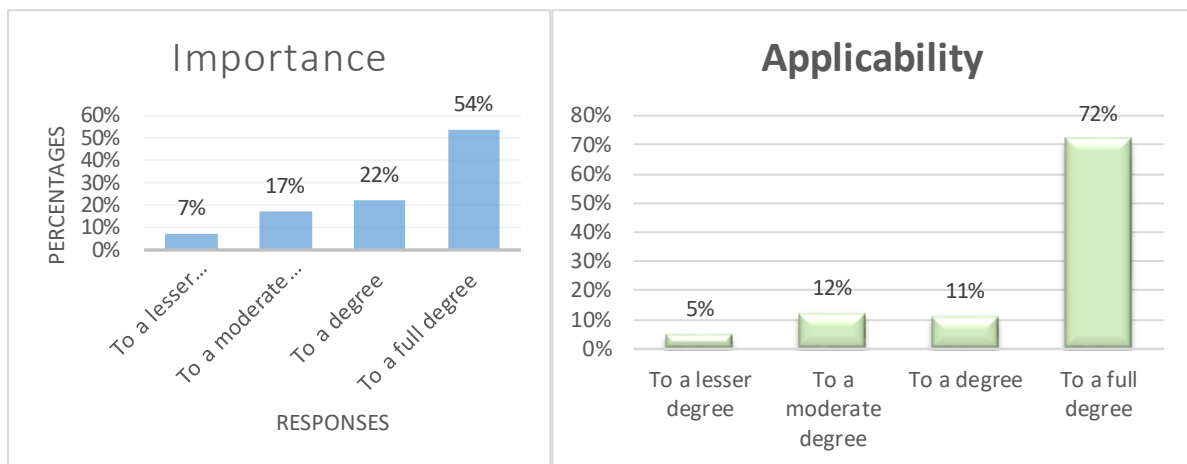


Figure 5.17: Cyber- security policy

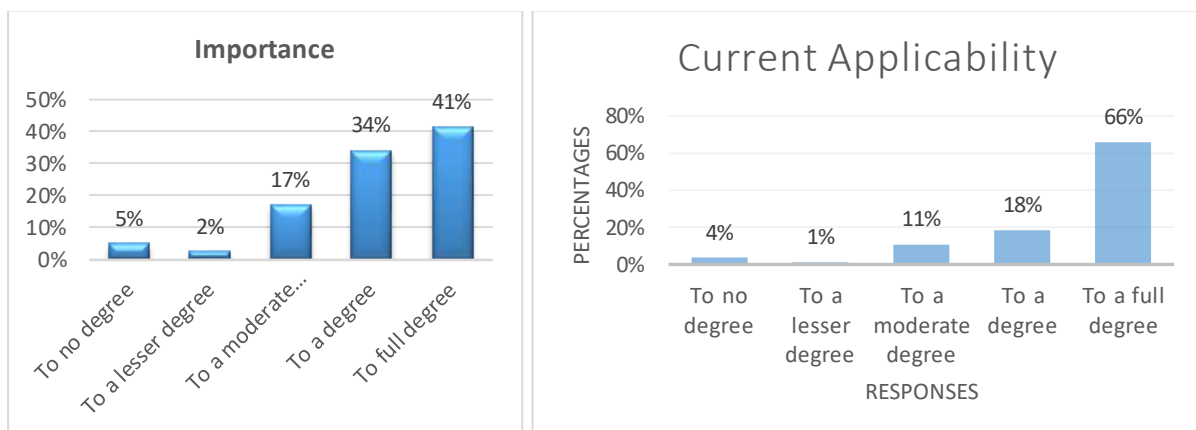


Figure 5.18: Communication programme

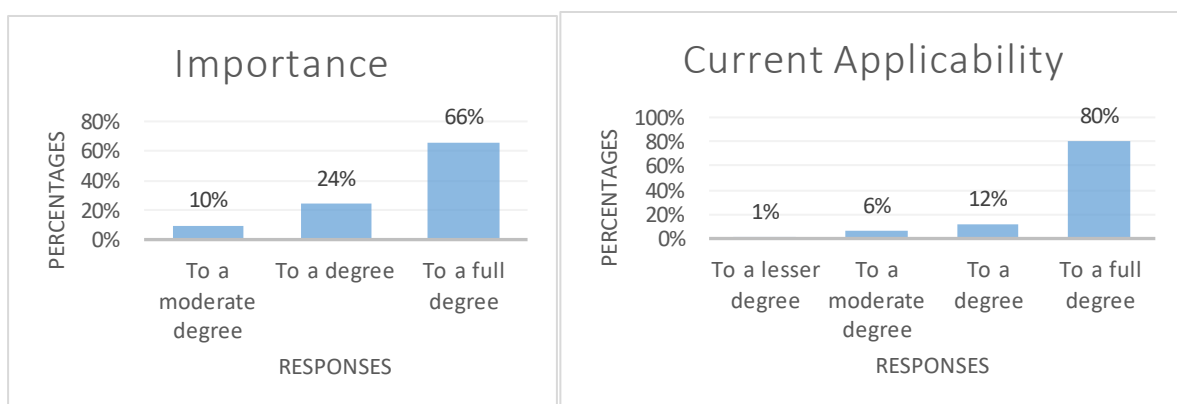


Figure 5.19: data back-up facilities

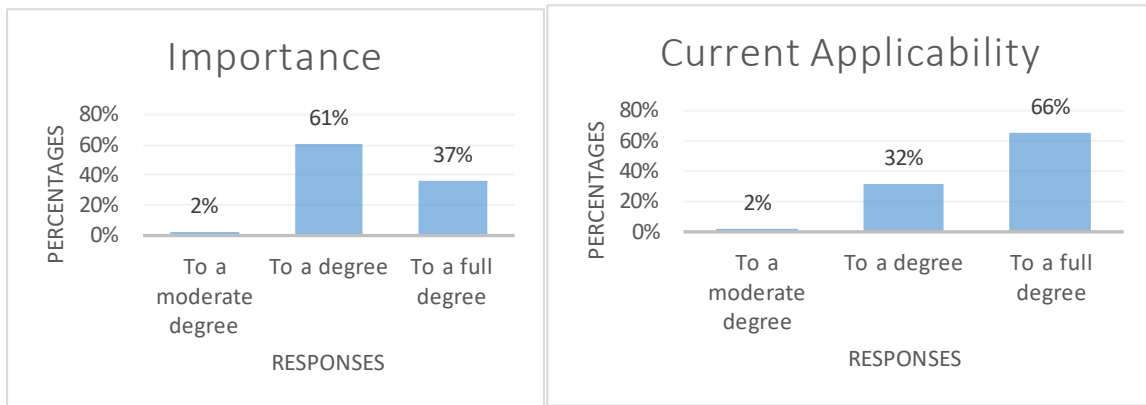


Figure 5.20 Business continuity management

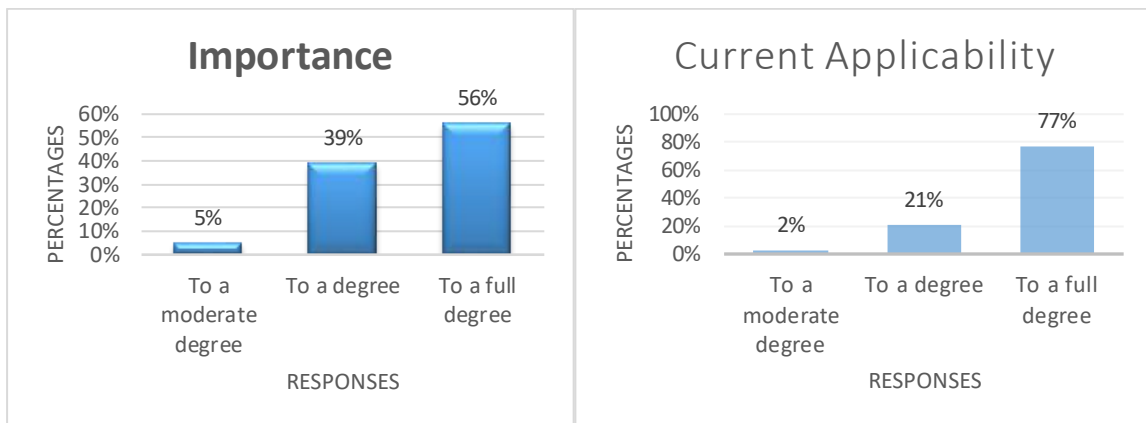


Figure 5.21: Inclusion of all stakeholders in BCM

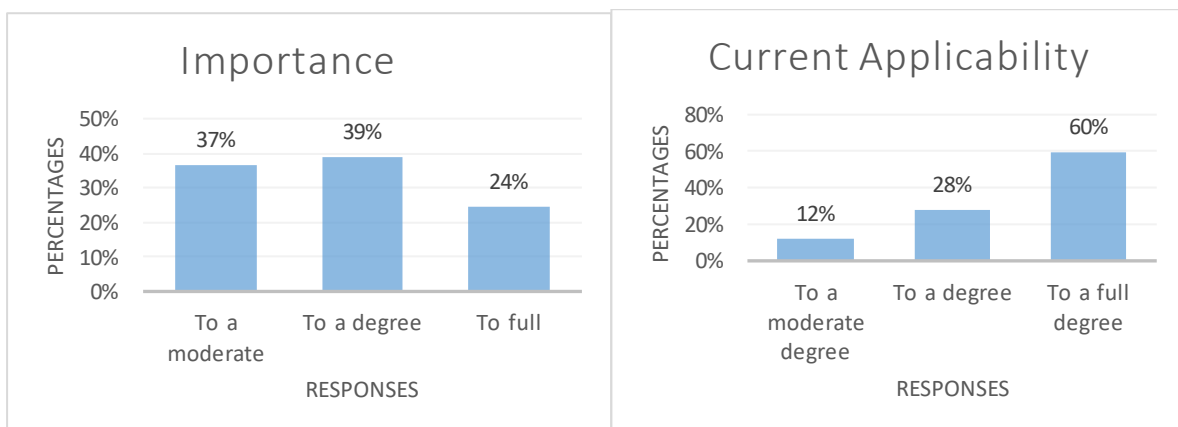


Figure 5.22 Crisis management

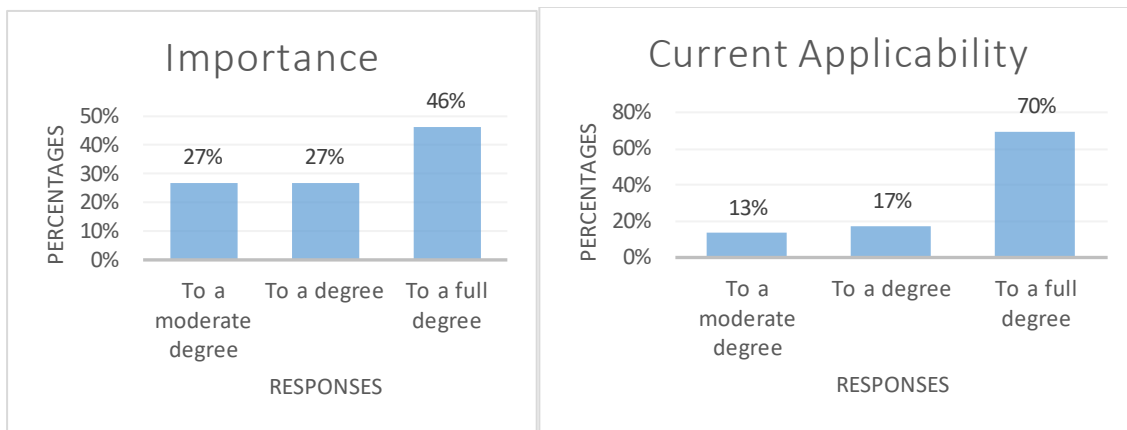


Figure 5.23: Business continuity plan (BCP)

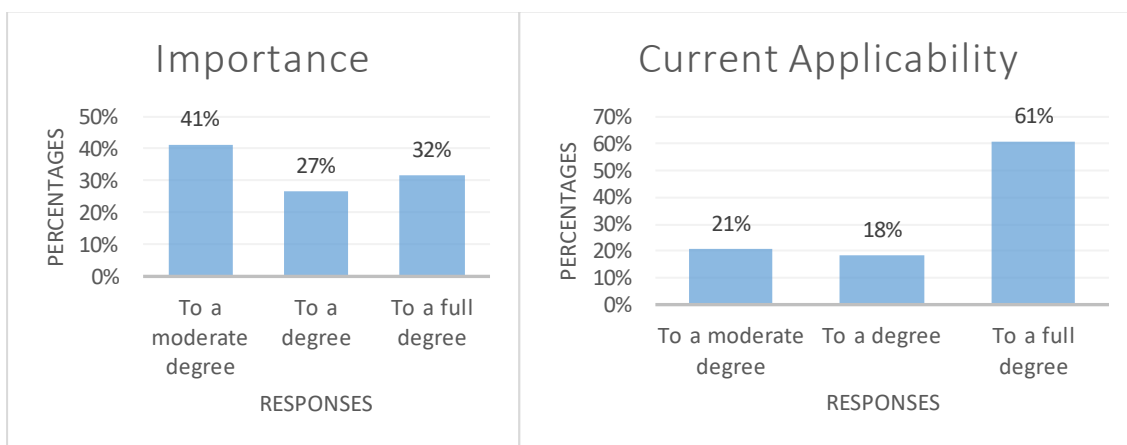


Figure 5.24 Training drills

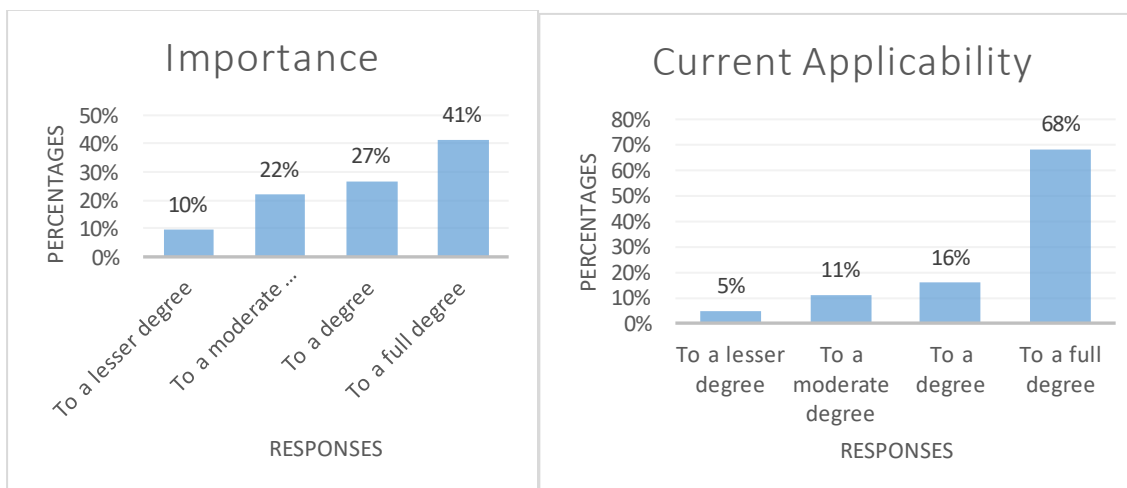


Figure 5.25: Identifying critical functions

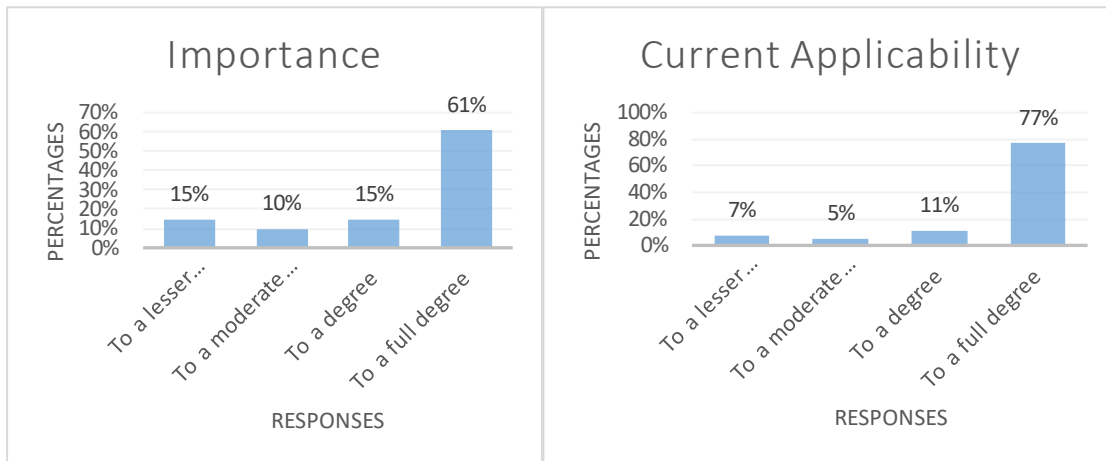
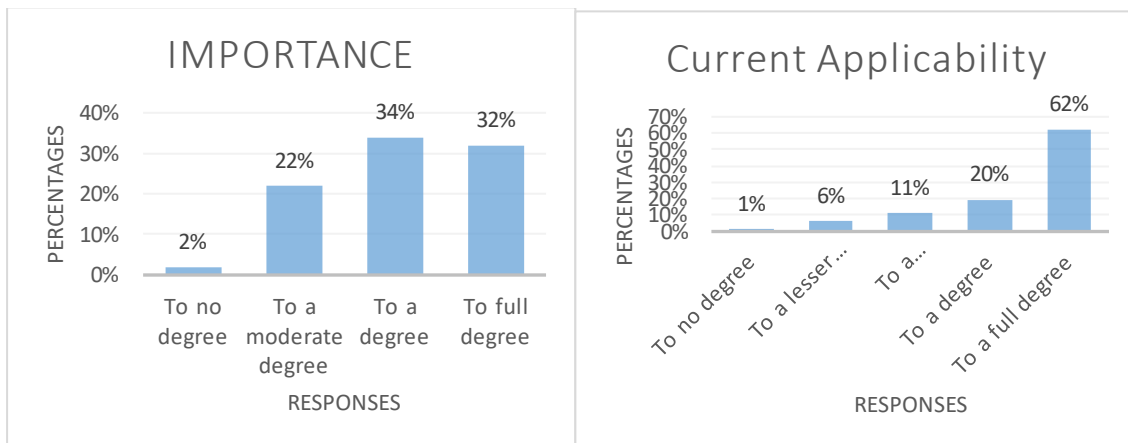


Figure 5.26: Remote working



Annexure I: Statistical results

	Group	Mean	Std. Deviation	Significance
Q1	Importance	4.93	.346	.000
	Current applicability	3.66	.693	
Q2	Importance	4.71	.901	.000
	Current applicability	3.80	1.054	
Q3	Importance	4.83	.381	.000
	Current applicability	3.59	.741	
Q4	Importance	4.78	.759	.000
	Current applicability	3.98	.935	
Q5	Importance	4.80	.459	.001
	Current applicability	4.37	.662	
Q6	Importance	4.90	.374	.001
	Current applicability	4.54	.596	
Q7	Importance	4.98	.156	.000
	Current applicability	4.51	.553	
Q8	Importance	4.88	.640	.002
	Current applicability	4.37	.799	
Q9	Importance	4.90	.300	.000
	Applicability	4.37	.767	
Q10	Importance	4.95	.218	.000
	Current applicability	4.05	.773	
Q11	Importance	4.80	.459	.000
	Current applicability	4.24	.830	

Q12	Importance	4.90	.300	.000
	Current applicability	3.88	.842	
Q13	Importance	4.93	.264	.000
	Current applicability	4.02	.790	
Q14	Importance	4.93	.346	.000
	Current applicability	4.29	.680	
Q15	Importance	4.90	.300	.000
	Current applicability	3.76	.767	
Q16	Importance	4.78	.690	.004
	Current applicability	4.22	.988	
Q17	Importance	4.78	.759	.001
	Current applicability	4.05	1.071	
Q18	Importance	4.88	.557	.003
	Current applicability	4.56	.673	
Q19	Importance	4.93	.346	.000
	Current applicability	4.34	.530	
Q20	Importance	4.98	.156	.000
	Current applicability	4.51	.597	
Q21	Importance	4.83	.381	.000
	Current applicability	4.12	.781	
Q22	Importance	4.93	.264	.000
	Current applicability	4.20	.843	
Q23	Importance	4.90	.300	.000
	Current applicability	3.90	.860	

Q24	Importance	4.95	.218	.000
	Current applicability	4.00	1.025	
Q25	Importance	4.93	.264	.000
	Current applicability	4.22	1.129	
Q26	Importance	4.88	.510	.000
	Current applicability	3.83	1.070	

Annexure K

Ke.Nna
Publishing Services



This certifies that the thesis "OPERATIONAL RISK CONTROL MEASURES FOR THE LESOTHO BANKING INDUSTRY TO MANAGE A CRISIS EVENT: A CASE STUDY OF COVID-19" was edited by Ms SehloDIMELA, who has over 10 years of scholarly publishing and editing experience.

The services provided include:

1. Ensuring accuracy in grammar and punctuation to improve readability and clarity
2. Consistency and structural enhancements to aid in creating a cohesive article

The editing was completed on 14 June 2024.

Ms SehloDIMELA is contracted by the University of South Africa's College of Economic and Management Sciences to provide academic editing services. She holds a Masters in TESOL.

FOR ANY ENQUIRIES RELATING TO THE ABOVE, SEE BELOW CONTACTS



CT SEHLODIMELA, MA(TESOL), PMP
Managing Director: Ke.Nna Publishing Services



Tshegofatso.s@outlook.com