Digitalisation of risk management in the South African banking industry: A case study of a major South African bank

Lambert Francois Gresse

2289117

2289117@students.wits.ac.za

+27 82 481 7667

A research report submitted to the Faculty of Commerce, Law and Management, University of the Witwatersrand, in partial fulfilment of the requirements for the degree of Master of Management in the field of Digital Business

Johannesburg, 2019

ABSTRACT

The research studies the impact that digitalisation has on banking in South Africa, how it impacts the inherent risk in the system and accordingly, how banks respond to those risks that digitalisation presents using digitalised risk response strategies.

The fourth industrial revolution has meant that the way in which banks are differentiating themselves from their competitors and what customers are demanding from them are rapidly changing. This is distinct from previous industrial revolutions as it is characterised by velocity, scope and systems impact. Companies are being exposed to disruptive technologies and with it comes increased complexity and risk. Therefore, there is an apparent link between digitalisation and risk management. The research aims to understand the impact of digitalisation on risk management and accordingly how banks should respond to mitigate those risks.

The research adopted a mixed method, case study approach. The research was conducted using online questionnaires and face-to-face interviews, with structured and semi-structured questions. The data collected from the questionnaires and feedback from participants in the interviews were then combined to draw a conclusion based on the findings.

Key findings and insights were that banks should revisit the methods and models used to perform risk management, as velocity plays an increasing role in the types of risk that disruptive technologies introduce. Furthermore, the role that staff members, their skills and the tools that they have access to, to respond to risks, needs to improve.

KEYWORDS

Risk management, Digitalisation, Impact, Likelihood, Velocity, Risk assessment, Risk response; Fourth Industrial Revolution

DECLARATION

I, Lambert Francois Gresse, declare that this research report is my own work except as indicated in the references and acknowledgements. It is submitted in partial fulfilment of the requirements for the degree of Master of Management in the field of Digital Business at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in this or any other university.

Name: Lambert Francois Gresse Signature: 

Signed at Centurion

On the 20th day of April 2020

DEDICATION

First and foremost, the research is dedicated to my partner, who has been extremely supportive throughout this journey. Thank you for your encouragement and confidence in me to get this done.

To all the people around the world currently dealing with the deadline pandemic known as COVID-19, peace and good health be with you.

ACKNOWLEDGEMENTS

I would like to acknowledge Dr Thanti Mthanti, my supervisor, for his knowledge, experience, and guidance throughout the process. Your support and patience to assist me in writing this paper are greatly appreciated.

Thank you to Ms Ayanda Magida, from Wits Business School for your guidance and assistance throughout the degree programme and research process.

To the various lecturers at Wits Business School who transferred knowledge to us so passionately, especially Prof. Brian Armstrong and Prof. Gregory Lee. Thank you!

To my employer for allowing me to take time out of the office to complete my studies and everyone who participated and contributed towards completing the surveys and interviews. It would not have been possible without you.

Finally, to my family and partner for your encouragement and support during this journey.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

3LoD	:	Three lines of defence
4IR	:	The fourth industrial revolution
AI	:	Artificial Intelligence
AR	:	Augmented Reality
BCBS	:	The Basel Committee on Banking Supervision
CEO	:	Chief Executive Officer
CRO	:	Chief Risk Officer
ERM	:	Enterprise Risk Management
GDPR	:	General Data Protection Regulation
HR	:	Human Resources
IoT	:	Internet of Things
IRMSA	:	The Institute of Risk Management South Africa
ISO	:	International Organisation for Standardisation
IT	:	Information Technology
ML	:	Machine Learning
POPIA	:	Protection of Personal Information Act
VR	:	Virtual Reality
WEF	:	World Economic Forum

1 INTRODUCTION

1.1 Purpose of the study

This research was conducted using a mixed-method study to explore how digitalisation impacts the risk management framework in the South African Banking industry. This research report examined the impact that digitalisation has on banking and how banks subsequently respond. It therefore also looked at the operational risk management process, in particular, the assessment of risks and subsequent risk response. The risk management process as defined by ISO31000 is depicted graphically, in Figure 1 below.

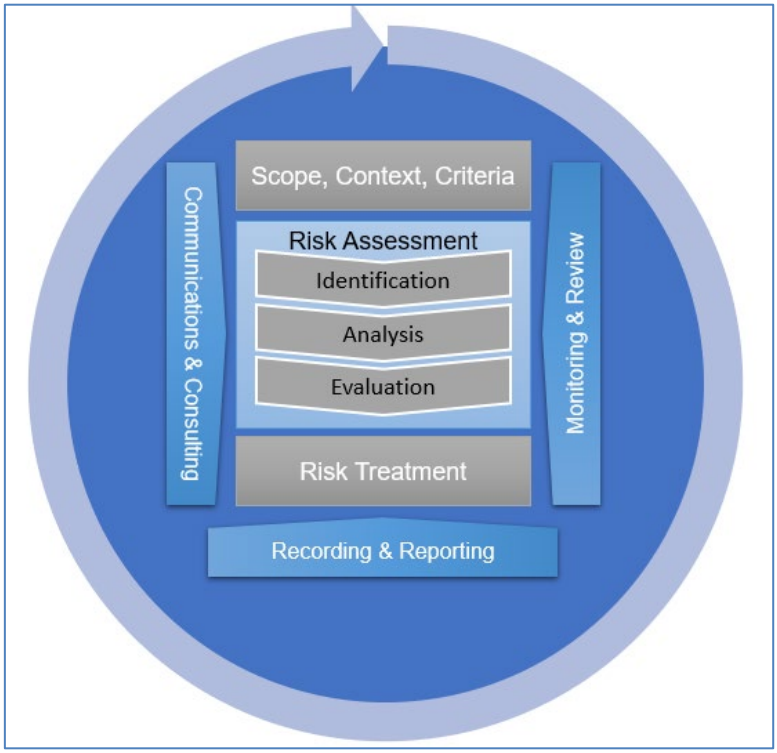


Figure 1: Risk management process according to ISO31000:2018 (International Organization for Standardization, 2018)

1.2 Context of the study

Bernstein (1996, p. 1), said that “The revolutionary idea that defines the boundary between modern times and the past is the mastery of risk: the notion that the future is

more than a whim of the gods and that men and women are not passive before nature." With this powerful quote, Bernstein implies that up until the point where people were able to identify and assess risks, people, in general, were vulnerable against the impacts or consequences of unfortunate events. Thus, in the absence of foresight, people and organisations were left exposed, where this situation could have been avoided with timeous response planning and action.

There are several risk categories including operational risk, market risk, regulatory risk, and credit risk to name but a few. This paper will focus on operational risks associated with financial institutions. Cruz, Coleman, and Salkin (1998) explain that operational risk (OR), is an important risk type for financial institutions. The different subcategories of OR will be elaborated on in the following chapters.

The paper examined, in the context of South African banking, the impact that digitalisation has on banking, how it impacts the inherent risk in the system and accordingly, how banks respond to those risks that digitalisation presents using digitalised risk response strategies.

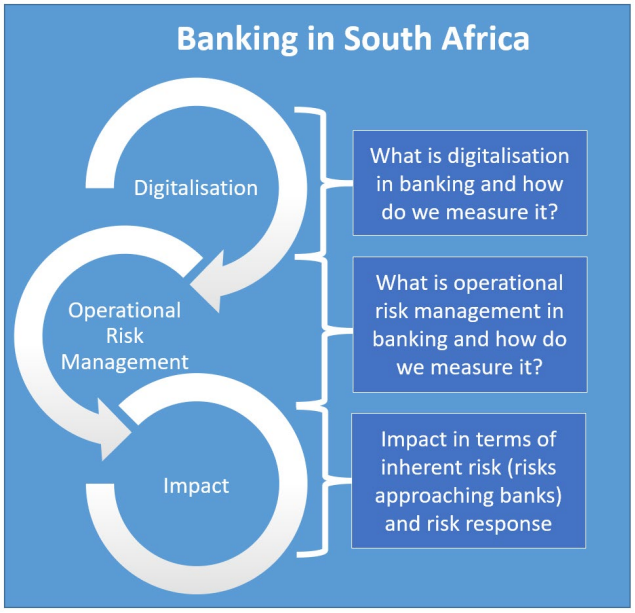


Figure 2: Graphic depiction of the context of the study

The departure point of the research is therefore that digitalisation has an impact on the inherent risks in banking, the way banks respond and what controls are being put in place to manage the residual risks down to acceptable levels. The impact and the

degree to which banks are ready to respond to these changes are being examined. Put differently, the paper looks at how digitalisation changes the operational risk landscape (inherent risk) in banking and in return, how banks are responding by changing the risk controls.

1.2.1 *Digitalisation and the 4th industrial revolution*

Professor Klaus Schwab first devised the term, the Fourth Industrial Revolution, in his book with the same title in 2016. Prof. Schwab, who is the creator and executive chairman of the World Economic Forum (WEF) describes a world wherein the way we interact with each other in our daily lives, digitally and physically, by using connected technology (Xu, David, & Kim, 2018).

Prof. Schwab states that the first three revolutions freed humanity from using animal power through mechanisation and steam engineering (first industrial revolution), enabled production on massive scales through assembly lines and mass production (second industrial revolution) and by bringing digital abilities to the world through computers (third industrial revolution).

He argues that the fourth industrial revolution (4IR), also known as Industry 4.0, is fundamentally different from the first three. It has unique characteristics in the digital technologies available today that creates a fusion between physical, digital and biological realms. These all create a world of disruption and possibility, across industries around the globe (Schwab, 2016). Refer to the graphic depiction below of the 4 industrial revolution phases.

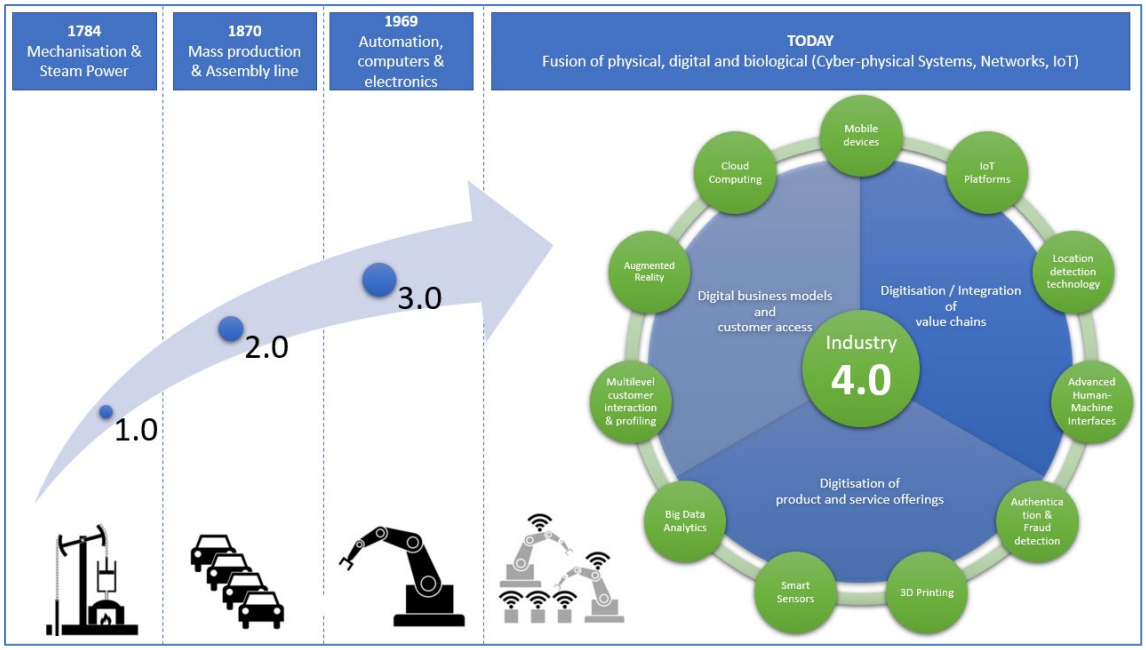


Figure 3: Graphic depiction of the four industrial revolution phases: Adapted from ICT Works (ICT Works, 2019)

Naturally, neither the banking sector nor South Africa as a country has remained untouched by this. South African President Cyril Ramaphosa indicated that the 4IR presents tremendous economic opportunities for South Africa and its people. The president indicated that the focus areas would be infrastructure and skills development (Ramaphosa, 2019). The banking sector has seemingly embraced the digitisation potential that has come with the 4IR.

1.2.2 *Banking in South Africa*

According to the South African Reserve Bank (SARB), the county's five largest banks comprised 90,5% of the South African Banking industry by asset value. These comprised of the following banks in order of decreasing asset value: The Standard Bank of South Africa Limited, FirstRand Bank Limited, Absa Bank Limited, Nedbank Limited and Capitec Bank Limited (South African Reserve Bank, 2018).

An increasing number of competitors banks have entered into the market, many of them adopting a new digital business model to challenge the more traditional banks in the form of Financial Technology firms, also known as Fintechs (The Centre of Excellence in Financial Services, 2019). These include Discovery Bank, Bank Zero

and Tyme Bank who have seemingly entered into the market to radically disrupt the industry leveraging digitalisation (Moyo, 2019).

1.2.3 *Digitalisation, Digital Banking and Digital Banks*

Traditional South African banks are hoping to reposition themselves strategically to compete with the influx of FinTechs in the country. The aim is to ensure that they remain relevant in the eyes of their customers in the face of rapid digitalisation of the South African banking industry (Coetzee, 2018). Leaders in the social media and online shopping space have also entered the fray. Facebook recently launched a cryptocurrency called Libra and online shopping giant Alibaba has seen success in the payments space since the launch of Alipay. Similarly, Vodafone's m-Pesa has seen success in sub-Saharan Africa to the point that it has outmatched traditional banks, especially in Kenya and Tanzania. Banks who do not embrace the wave of digitalisation face the risk of becoming irrelevant in their customers' eyes. They need to accelerate their move towards digital transformation, or they will find themselves being left behind in a high-risk, low-return and capital-intensive group of role-players while digital giants usurp customers and profits in the market. Senior managers in traditional banks may state that they embrace digital transformation, but few banks have really demonstrated how they leverage big data, analytics, and AI to the benefit of the organisation or its customers. It also remains to be seen how banks aim to attract and retain top talent to enable this journey in the likes of engineers, data scientists and user experience designers (Kumar et al., 2019).

The term digitalisation is extremely broad and refers to the way the bank enables its customers to conduct banking using digital means. It relates to both products and services that banks offer and it is typically accessed using personal computers and increasingly more, smart mobile devices. The key benefits from a user perspective talk to speed, ease of access and having a variety of options available to bank digitally. This means that not only are products and services shifting towards digitalisation but so are the internal operations of banks (Sreedhar, 2018). Simply put, products and services that are digitalised describe the *digital business*, i.e. the way in which customers transact and interact with the organisation. Digitalising internal operations

talks to *digitalisation within the business*. The two concepts differ and therefore carries different levels of risk and require different risk response strategies.

Instead of isolated initiatives, banks need to adopt a holistic approach towards digitalisation. This means that the strategy needs to be driven from the top requiring an interlinked strategy across the organisation. Banks need to ensure that they digitise the end-to-end customer journey to achieve scale and oust the competition. Key to achieving this is leveraging big data, analytics and AI (Kumar et al., 2019).

The degree to which banks find themselves ready to embrace the digitalisation journey may determine how prepared they are to respond to the associated risks that digitalisation brings, such as handling large volumes of data or ensuring cybersecurity resilience. Perhaps the biggest risk is failing to recognise that digital transformation is necessary to remain relevant, profitable and competitive. To determine if a bank is fit for the future, a few diagnostic questions may be asked to assess this. This ranges from the degree to which a bank is digitally enabled, or fit for the future, relative to its competitors.

Together with the digital strategy for the business, as determined by the board and the CEO, the Chief Risk Officer (CRO) plays a pivotal role too. Imperative to the success of the strategy is that a digital risk strategy is set as well. The end-to-end operations of the bank are changing and as the ecosystem transforms, so too must the functions such as risk transform (Grasshoff et al., 2019; Kumar et al., 2019).

1.2.4 *Risk management in Banking*

Risk traditionally comprises of two components, namely the probability or likelihood of "failing to achieve an outcome" and the impact or consequence of "failing to achieve that outcome" (Defense Systems Management College, 2001). Put differently, "risk is a financial measure of the impact of a failure *x* the probability of an event occurring" (Stoneburner, 2006; Sumner, 2009).

These two dimensions have traditionally defined the risk model for assessing risk, but in the digitally transformed environments where speed is of the essence, a third dimension needs to be added, i.e. velocity or speed of onset of risk. This is what is

suggested by Quan and Chiang (2017), whereby risk needs to be expanded to include velocity to ensure risk and uncertainty management in a high-velocity environment.

A fourth dimension has been suggested by Curtis and Carey (2012), who suggested that in addition to Impact, Likelihood and Velocity, Vulnerability needed to be added to the equation. Vulnerability refers to how prone an organisation is to a risk event as determined by their preparedness, agility and adaptability (Curtis & Carey, 2012).

The financial disasters seen in the global financial crisis of 2008 have increased the need for various forms of risk management. Though the fact that firms can get themselves into trouble is not a new concept, the rapidity at which it now happens is novel (Pyle, 1999). The global financial crisis has largely been a catalyst to transformation in banking, where the biggest changes that have been observed were around regulations. The next decade, however, sees the risk management function in banking transforming with specific trends around digitalisation shaping the future of the function (Härle, Havas, & Samandari, 2016).

Digital transformation has led to rapidly changing business environments, not just in banking but across industries. This has paved the way exponential opportunities as it relates to capabilities, new initiatives and innovation. Together with the digital transformation journey, it is crucial that banks also manage risks that are introduced and its associated impact on the existing business environment. Regardless of all the challenges and risks the transformational environment presents, banks cannot deny the opportunities that it offers (Mahajan, Parthasarathy, & Jain, 2018).

Digital risk refers to the risk associated with digital transformation and new digital business processes and business models. It is the risk associated with new and unexpected consequences of digital transformation and requires the involvement of not just technology executives, but more importantly the buy-in from business executives (Digital Risk Management Institute, 2019; RSA Security, 2019b).

Digital risk varies from one organisation to another, depending on how it integrates digitalisation into its business model. This depends on the level of digitalisation within the business or the level of digitalisation it presents to its customers through products and services. The core deviation from traditional risk is the speed of onset of the risk or the velocity. Digital risk manifests itself in the organisation through three different

categories of traditional risk. These are strategic risk, operational risk and governance risk (Deloitte, 2019).

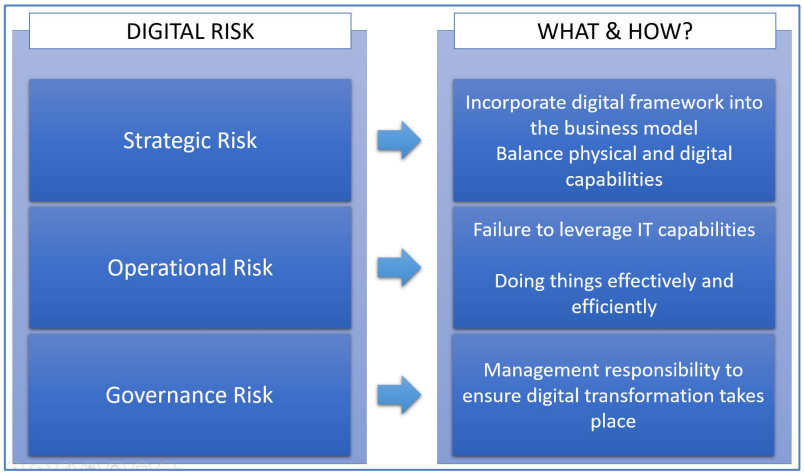


Figure 4: Manifestation of digital risk inside the organisation (Deloitte, 2019)

Strategic risk is the risk that an organisation faces as a result of poor decision making, substandard execution of decisions or failure to respond to a changing business environment (BusinessDictionary, 2019). In the context of digital risk, strategic risk is centred around companies not having successfully integrated the digital framework into their business model. They have not embarked on a digital transformation journey and therefore stand the risk of disintermediation and seeing an exodus of customers.

Digital operational risk is a threat that an organisation faces as a result of not implementing digital solutions to improve efficiency and productivity. This may, for example, include the lack of utilising big data and analytics for decision making or not using AI and robotics for customer service processes in a bank. Mere automation of processes is not sufficient, and the fundamentals of the business model need to transform in order to avoid digital risk within its operations.

Governance risk is a result of both the strategic and operational strategies and management needs to ensure that digital technologies are employed to successfully address the business model needs (Deloitte, 2019).

Operational risk is described as being closely related to human error, system failure, fraud and inadequate procedures and controls (Cruz et al., 1998). The Basel Committee on Banking Supervision (BCBS) (2006), defines operational risk as “the

risk of loss resulting from inadequate or failed internal processes, people and systems or from external events" (Basel Committee on Banking Supervision (BCBS), 2006, p. 144). The BCBS acknowledges that operational risk is an overly broad term and can take on different meanings. For this reason, financial institutions are allowed to adopt their own definitions, provided that the minimum standards as per the Basel definition are met. The following seven event types categories are acknowledged by Basel Committee on Banking Supervision (BCBS) (2006) in terms of operational risk:

i. Internal Fraud: Misappropriation of assets, tax evasion, intentional mismarking of positions, bribery.
ii. External Fraud: theft of information, hacking damage, third-party theft and forgery.
iii. Employment Practices and Workplace Safety: discrimination, workers compensation, employee health and safety.
iv. Clients, Products, and Business Practice: Market manipulation, antitrust, improper trade, product defects, fiduciary breaches, account churning.
v. Damage to Physical Assets: Natural disasters, terrorism, vandalism.
vi. Business Disruption and Systems Failures: Utility disruptions, software failures, hardware failures.
vii. Execution, Delivery, and Process Management: Data entry errors, accounting errors, failed mandatory reporting, negligent loss of client assets (Basel Committee on Banking Supervision (BCBS), 2006, p. 319).

It is essential that the risk function is enabled to anticipate, assess and monitor the digital risk environment that digital transformation within the organisation brings. These are new risks that present itself due to the digital transformation journey. This means that across the seven categories of operational risk, banks need to respond accordingly using digitally enabled skills and tools to minimise the risk, both to existing risks and the new digital risks.

1.3 Research problem

The 4IR is bringing about changes that are amplified both in speed and measure. These changes will impact social and economic constructs in society. The benefit can

only be created by ensuring that industries, like banking, are prepared and knowledgeable about the imminent impact of digitalisation (Xu et al., 2018).

Xu et al. (2018) explain that 4IR is not just an extension of the third industrial revolution. They propose that the 4IR is distinct in relation to velocity, scope and systems impact. It, therefore, seems almost apparent that the association between digitalisation and risk management needs to be understood and studied. The impact that digitalisation has on how fast risks are approaching banks versus how effectively and timeously they can respond, needs to be understood. Perhaps, more importantly, if traditional banks and FinTech's have not yet considered the impacts that digitalisation has on their business models, then they might find themselves in a disadvantaged soon.

At the centre of banking strategy going forward will be the way in which banks will benefit from new opportunities that digitalisation brings, but also how they mitigate the risks that this will impose (Rossi, 2017). In as little as six years from now, the risk functions in the banking industry would have to be drastically different from what they are today. These trends are shaped by multiple sources emanating from digitalisation and the 4IR (Härle et al., 2016). One of these sources is a direct result of customer demand. Clients are actively seeking out digital experiences when dealing with their banks (Cairns, 2017).

The impact of digitalisation on risk management in banking means that many South African banks may find themselves unprepared for the effects thereof in the near future. This result in the materialisation of digital risk within the organisation. Banks need to implement plans to prepare for this. They need to understand the inherent risk to their organisations and at the same know what is required to mitigate those risks. This research investigates ways in which such preparation may lessen the risks of digitalisation but how preparedness may also become a competitive advantage.

The research, therefore, aims to understand the impact of digital risk, i.e. failing to digitally transform and in turn understand the digitalisation of operational risk management to sufficiently respond to digital risk.

1.4 Research objectives

The objective of this research is to assess the impact of digitalisation on the risk management function in the South African Retail Banking industry. This is to better understand the level of perceived preparedness that exists amongst banks while South Africa is in the midst of the 4IR and digitalisation of products and services is at the forefront of the strategy of both traditional banks and FinTechs.

Sub objectives:

1. Preparedness of banks for the inherent risk associated with digitalisation.
2. Readiness to respond accordingly to the inherent risk associated with digitalisation.

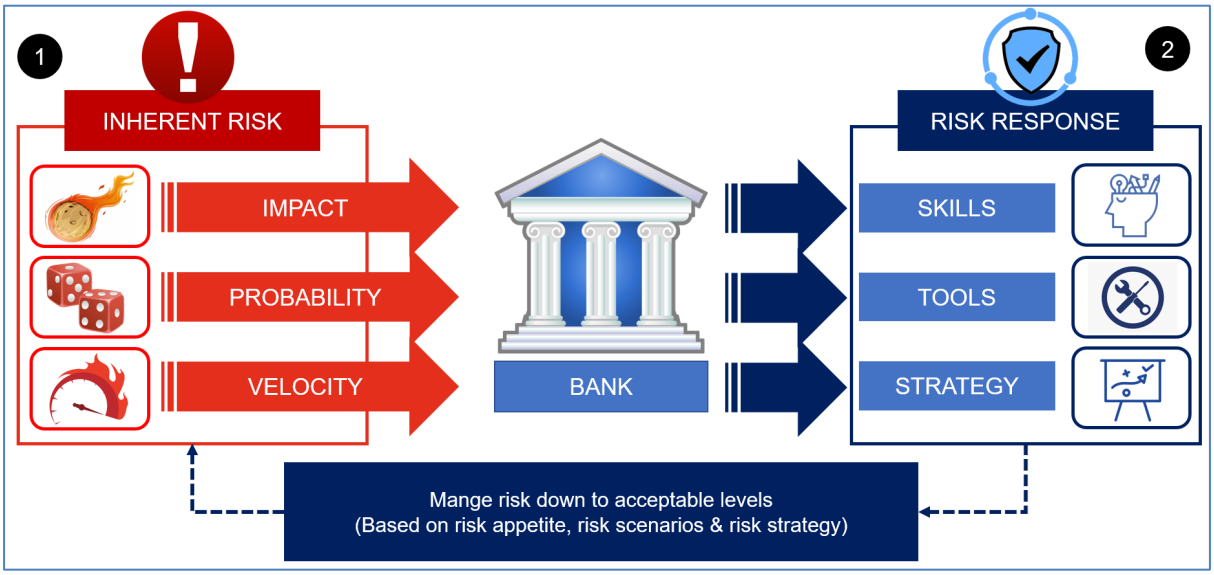


Figure 5: Graphic representation of the research objectives

Figure 5 depicts the calculation of inherent risk, i.e. the level of risk the bank would face in the absence of any control being applied to manage the residual risk down to acceptable levels. Residual risk, i.e. the risk that the bank is faced with after responding to the risk by applying skills, tools and strategies, should be within the risk appetite of the bank and in line with the risk scenarios and strategies of the bank.

If the residual risk is equal to the inherent risk, it implies that insufficient controls have been formulated as part of the risk response. This is an ongoing, cyclical process and

not static. It evolves over time as the banks' strategy and business environment change.

1.5 Significance of the study

The significance of the study is to draw parallels between the inevitable advent of digitalisation in banking, the inherent risk that it present and the degree to which banks in South Africa are prepared to respond. In doing so, the impact that this will have on the retail banking industry may be better understood and recommendations can be made for better preparedness and may lay the foundation for future research.

What is not clear is whether the industry as a whole is prepared for the impact of digitalisation and more so, do they perceive it to be a threat or enabler for their businesses. The risk culture in the South African banking is fairly mature (IRMSA, 2019), but the digital risk maturity of it is not yet known. In a digital economy, the rails on which the economy runs need to be stable enough to withstand the knocks and challenges which carries it forward.

1.6 Delimitations of the study

The research is focussed on commercial banks in the South African Banking industry and does not include mutual banks, investment banks or development and land banks.

The research focusses purely on the operational business risk function and it does not include the broad spectrum of risks such as credit risk, market risk, liquidity risk, etc.

Vulnerability as the fourth dimension of risk assessment is not being researched as part of this study. This dimension has been proposed by Curtis and Carey (2012), but only the three-dimensional model is looked at, i.e. impact, likelihood and velocity.

1.7 Definition of terms

Digital Business Transformation: "Digital business transformation is the process of exploiting digital technologies and supporting capabilities to create a robust new digital business model" (Gartner, 2019).

Digitalisation: “Digitalisation is the use of digital technologies to change a business model and provide new revenue and value-producing opportunities. It is the process of moving to digital business” (Gartner, 2019).

Digitisation: “Digitisation is the process of changing from analogue to digital form, also known as digital enablement. Digitisation takes an analogue process and changes it to a digital form without any material changes to the process itself” (Gartner, 2019).

Risk: “Effect of uncertainty on objectives” (International Organization for Standardization, 2009).

Risk Analysis: “process to comprehend the nature of risk and to determine the level of risk” (International Organization for Standardization, 2009).

Risk Assessment: “overall process of risk identification, risk analysis and risk evaluation” (International Organization for Standardization, 2009).

Risk Attitude: “Organization's approach to assess and eventually pursue, retain, take or turn away from risk” (International Organization for Standardization, 2009).

Risk Evaluation: “Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable” (International Organization for Standardization, 2009).

Risk Identification: “Process of finding, recognizing and describing risks” (International Organization for Standardization, 2009).

Risk Management: “Coordinated activities to direct and control an organization with regard to risk” (International Organization for Standardization, 2009).

Risk Management Framework: “set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization” (International Organization for Standardization, 2009).

Monitoring: “Continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected” (International Organization for Standardization, 2009).

1.8 Assumptions

1. Risk management is embedded in the banking industry of South Africa, as all boards are guided by King IV principles of sound corporate governance.
2. Banks adopt the same approach towards risk management in terms of lines of defence, i.e. business as first-line, risk management as second-line and internal audit as the third-line.
3. Due to an increase in digital banks and Fintechs, all retail banks in South Africa are on a digital transformation journey to remain competitive.

2 LITERATURE REVIEW

2.1 Introduction

The purpose of the chapter is to introduce the literature that has been reviewed as part of this study. The research study aimed to understand the implications or impact of digitalisation on risk management in South African banking.

Literature that has been reviewed was gathered from different sources. These comprised of:

i. Primary sources: Seminal artefacts, academic journals, speeches, market research, case studies, government documents.
ii. Secondary sources: Academic journals, magazine articles, textbooks, conference proceedings.
iii. Tertiary sources: Dictionaries, guidebooks, manuals.

To understand the impact that digitalisation has on risk management in banking, the association between digitalisation and the strategic implication to banking needs to be understood. The bank will derive its enterprise risk management (ERM) strategy from its business strategy and therefore these two are interlinked. By association, strategic implications will impact the ERM strategy of the business.

From here on, the research addresses each sub-objective as it relates to preparedness in the inherent risk associated with digitalisation, appropriate risk responses and changes in risk attitude and risk response strategies.

The focus of the literature review is to understand the preparedness amongst banks for the 4IR and digitalisation, how they have begun to prepare to respond accordingly to the changing business and risk landscapes and how this impacts their strategies around risk identification, monitoring and control.

2.2 The strategic implication of digitalisation on banking

Innovation in banking is happening at an unprecedented and accelerating pace. New technologies combined with digital strategies and new business models, sees the face

of banking changing in an ever more demanding space driven by customers increasing need for digital banking solutions. Many factors are driving the tides of change including customer needs, new digital technologies and cybersecurity and risk management (Weichert, 2017).

According to Rogers (2016), there are five domains that organisations need to focus on to ensure that they digitally transform themselves. These are made up of customers, competition, data, innovation and value. The customer domain talks to how the organisation harnesses its customer networks. The competition domain addresses the need to go beyond a product mindset and immerse the company strategy into platform thinking. The data domain talks to leveraging data as a strategic asset and the innovation domain talks to the need for rapid experimentation and prototyping. Finally, the value domain talks to the evolution of the organisation's value propositions.

Ultimately, digital transformation is rapidly changing the way in which organisations think about their infrastructure needs, marketing strategies and business models (RSA Security, 2019a). The strategies that banks in South Africa will adopt over the next ten years, will define their ability to remain relevant and their ability to compete in this rapidly evolving space (Coetzee, 2018).

The digital revolution has seen organisations being penetrated by a myriad of new technologies and concepts. These include augmented and virtual reality (AR/VR), robotics, big data and analytics, cryptocurrencies and blockchain technologies, artificial intelligence (AI) and the internet of things (IoT) to name but a few. In South Africa, customers have seen both traditional banks and Fintechs adopting these technologies.

Probably one of the most visual, physical world examples of this, was the introduction of a humanoid in Nedbank's branches. The robot was called "Pepper" and was built by Japanese corporation Softbank. Pepper can be encoded to acknowledge fundamental human emotions and have conversations and interactions with customers (Khumalo, 2018). Nedbank sees the exploration into AI and robotics as the first steps towards what would ultimately become a significant part of their strategy and customer offerings. Nedbank stated that they intend to not just embrace, but to

lead in digital, especially with new Fintech entrants like Bank Zero, Tyme Bank and Discovery Bank all entering with a digital-first strategy (Doyle, 2018; Khumalo, 2018).

Banks have started to use automation, AI and robotics to improve the response time and address the need from customers demanding an always-on customer experience. Algorithms are replacing traditional investors, making investment decisions using complex data-driven models (BusinessTech, 2017). Even call centres are seeing human staff being replaced with chatbots, essentially replacing the need for a person to man the line on an ongoing basis and the customer would not even be aware of the fact that they are conversing with a robot (Barapatre, 2019).

Banks are adopting digital technologies, not just because customers are demanding it but also to reduce errors and therefore limit the financial risk exposure. A single event can lead to millions of Rands worth of losses, not to mention reputational damage (Barapatre, 2019). Banks are also embracing big data and analytics as a means to make better decisions. Advancements in data science and machine learning have allowed organisations of all sizes to leverage rich data analytics giving organisations unprecedented insight into their customers and markets (Ismail, Malone, van Geest, & Diamandis, 2014; Weichert, 2017). The benefits that big data presents have been referred to as the 5P's, i.e. productivity, prevention, participation, personalisation and prediction (Ismail et al., 2014, p. 80). It has however been noted that as the use of big data and the economic benefits grow, so too will the risk and challenges (Manyika et al., 2011).

2.3 New technologies, concepts and emerging risks

Digitalisation has not just brought along benefits to banks and their customers, associated risks have also increased. Cybercrimes are on the rise and at the same time regulators are clamping down on banks and organisations to ensure that customers are protected.

In South Africa and Europe, regulations such as the Protection of Personal Information Act (POPIA) and General Data Protection Regulation (GDPR) have become top of mind for banks to ensure data privacy for customers and organisations, in the face of rising cybercrimes and data breaches. Most recently, the Cybercrimes and

Cybersecurity Bill has been drafted and aims to create offences and impose penalties which have a bearing on cybercrime (Department of Justice and Correctional Services, 2017). Data, however, does not only carry regulatory and cybersecurity concerns.

Big data has brought along the promise of being the biggest differentiator amongst competitors in recent years. A common framework has emerged, whereby big data is typically classified along three dimensions, namely volume, variety and velocity (Chen, Chiang, & Storey, 2012; Gandomi & Haider, 2015). Data mining and big data have specifically been acknowledged as a tool that assists the banking industry to perform fraud detection and therefore enhance security, as well as assist with risk management activities (Hassani, Huang, & Silva, 2018). It has been accredited with assisting banks in faster response times to combat specifically phishing attacks, fraud, money laundering and breaches in online and mobile security.

Furthermore, along with data analytics, machine learning (ML) and artificial intelligence (AI) have been credited with assisting risk managers making faster and more informed decisions when responding to risks. Machine using algorithms to process data at great speed and in large quantities enables risk managers to rely on outputs far more superior to that of humans analysing the same risk trends and patterns (Aziz & Dowling, 2019). The increased risk associated with volume, variety and complexity of operational risk exposure amongst banks, has paved the way for AI and ML-based applications (Choi, Chan, & Yue, 2017). This is especially important for digitally transforming institutions that operated in more complex environments, both as part of running the banks operations and the customer-facing applications that they develop in cyberspace.

Cyberspace can be defined in terms of four layers namely, physical, logical, information and people layers and possesses three characteristics namely connectivity, speed and storage (Clemente, 2015). Connectivity talks to devices and “things” being connected to exchange information, speed talks to the processing power of devices and storage revolves around where and how information and data get stored, e.g. physical drives or in the cloud. The benefits that these hold to desirable business and personal users are evident. The risk is that it cannot be ringfenced and as a result is also available to malicious users. The benefits that cyberspace lends the banking systems is undisputed, yet it brings with it very high inherent risks that are

costly to manage and mitigate. On top of that, data breaches and placing customers' data at risk does not only carry high reputational damages but also incurs massive regulatory fines and penalties.

The regulatory change is however inevitable and the same can be said for the wave of digitalisation in the midst of the 4IR. The question now remains to what degree banks are willing to take on risks in the pursuit of achieving their business objectives. How are they going to cope with this onset of digitalisation and the associated risks? If banks are going to put digitalisation at the centre of their business strategies, they need to ensure that the support functions to their business are enabling. This means that human resources (HR), IT, Finance and Risk Management, all need to have supporting strategies to meet the business strategy.

2.4 Top 12 risks South Africa will face in 2020

In their latest country risk report for South Africa, The Institute of Risk Management South Africa (IRMSA), identified the top 12 risks that the country would be facing going forward (IRMSA, 2020). Almost a quarter of the respondents came from the financial services sector in South Africa.

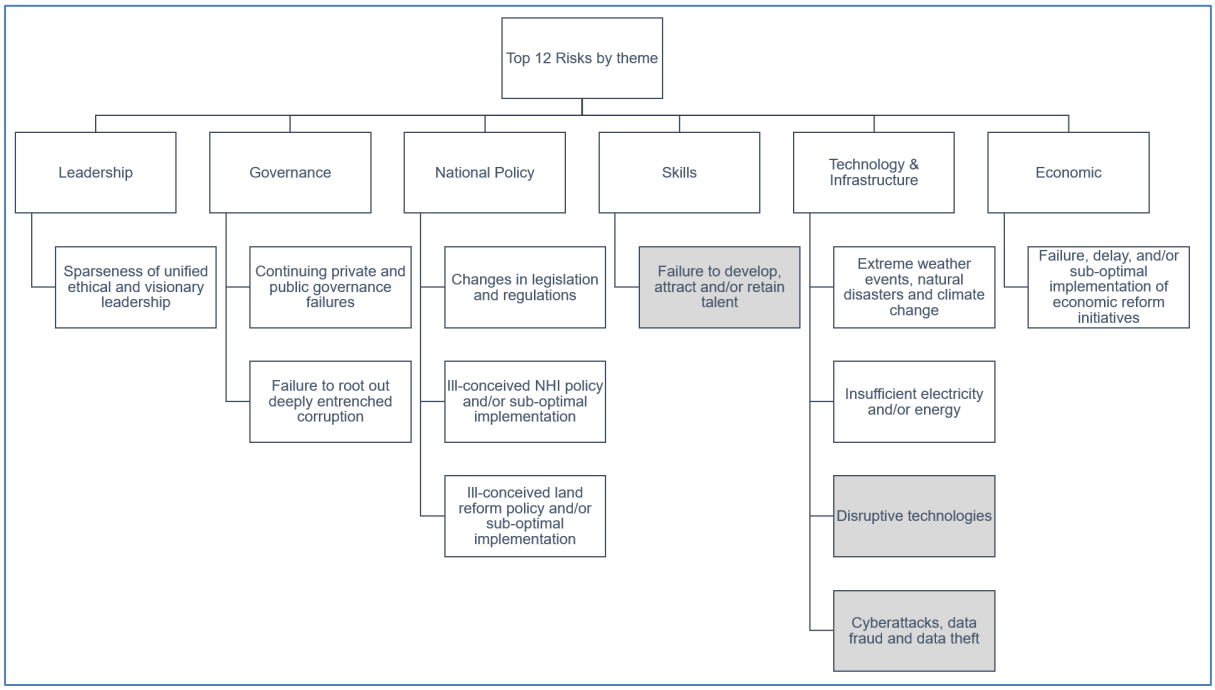


Figure 6: Top 12 risks - South Africa 2020 (IRMSA, 2020)

The risks in the report are grouped according to six themes. Two of these themes are also being discussed in this paper as they contributed directly towards the impact of digitalisation of risk management in the South African banking industry. More specifically, three of the risks identified talks to the two research propositions that is being discussed later on in this chapter, namely:

i. Failure to develop, attract or retain talent.
ii. Disruptive technologies.
iii. Cyberattacks, data fraud and data theft.

These are each discussed in more detail.

2.4.1 *Failure to develop, attract or retain talent*

The report highlighted the ineffective national education system and also noted that while South Africa is struggling to get to grips with the basic educational requirements, elsewhere in the world people are starting to exploit the benefits of the 4IR and various new technologies (IRMSA, 2020).

2.4.2 *Disruptive technologies*

Organisations may fail to grasp the gravity and scope of disruptive technologies, and they may fail to realise the risk until it is too late to manage or respond to those risks. There are only a handful of individuals that really appreciate the enormity associated with risk and disruptive technologies (IRMSA, 2020).

2.4.3 *Cyberattacks, data fraud and data theft*

Advances in technology and escalating complexity in organisations may result in escalating cybercrime activities and thereby harm the organisation. As technology becomes a more regular part of our daily lives, cyber-attacks will increase in frequency both on individuals and businesses (IRMSA, 2020).

2.5 The inherent risk associated with digitalisation (Risk assessment)

Organisations that will successfully digitally transform themselves, are the ones that embrace incremental innovation and experimentation (Ismail et al., 2014; Rogers, 2016). Traditional thinking needs to be re-evaluated and risk needs to be understood and embraced to successfully transform your organisation. Organisations that have high-risk intolerance levels will find themselves in an uphill battle when competing with other exponential organisations (Ismail et al., 2014). Risk aversion presents one of the biggest threats to innovation in a digital organisation (Rogers, 2016). It is therefore important to understand the risks and ensure that the organisation is prepared for what is lying ahead on the digital transformation journey and to ensure that risk appetite levels are set correctly to ensure calculated risk taking.

The banking industry was not only among the pioneering sectors to grasp the benefits associated with digital transformation, but also one of the industries to acknowledge the risks associated with it (RSA Security, 2019c). If this is indeed the case, then the question needs to be asked if South African banks are prepared for the inherent risk associated with digitalisation. Throughout the journey of digital transformation, the velocity and impact of risk associated with connectivity will drastically increase the need for rapid decision making and responsiveness (RSA Security, 2019c).

This means, that the usual methods of qualitative risk assessments need to be revisited. At this stage, it may be assumed that the three dimensions of risk assessment, i.e. impact, likelihood and velocity will all drastically change and that the gap between the two illustrates the risk associated with digitalisation for the organisation.

As part of the risk assessment, the research will look at the effects of digitalisation on the impact (consequence) and likelihood (probability) as well as the velocity (speed of onset) dimensions of risk measurement. Quan and Chiang (2017) expressed this in a mathematical formula, i.e. Risk = (Impact x Likelihood) + Velocity. This is graphically represented in Figure 7 below.

Risk as a product of Impact and Likelihood typically gets expressed in a 3x3, 4x4 or 5x5 matrix depending on the organisation's philosophy and needs. The figure below depicts a typical 5x5 risk matrix, where colours are commonly used to illustrate the inherent risk rating of the combined effect of impact and likelihood, typically expressed verbally as low, medium, high, very high and extreme.

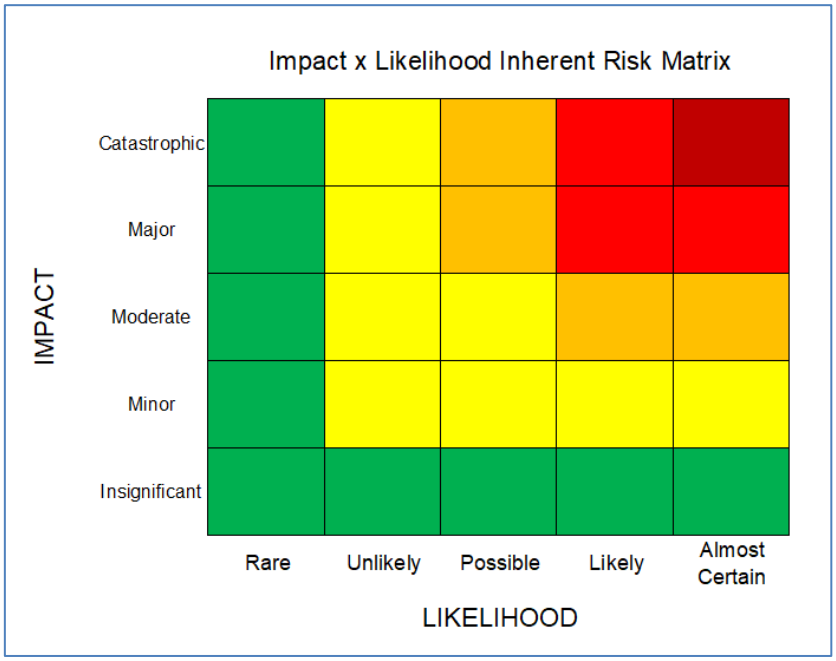


Figure 7: Risk matrix (Heatmap) (Adapted from Quan and Chiang (2017))

When the third dimension gets introduced, the complexity of the model naturally increases. Quan and Chiang (2017), suggested the following model as depicted in the figure below. It shows the 5x5 matrix in the figure above in a linear format, still expressing the mathematical equivalent of the risk rating on a scale ranging from 0 to 25.

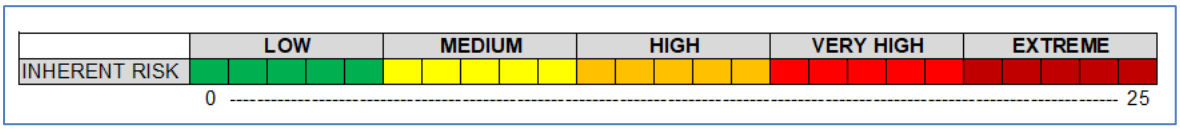


Figure 8: Linear matrix showing impact, likelihood (Adapted from Quan and Chiang (2017))

By using the linear model, the third dimension of velocity can now easily be added to express the mathematical formula of “(Impact x Likelihood) + Velocity”. Note that the scale now changes from 25 to 30.

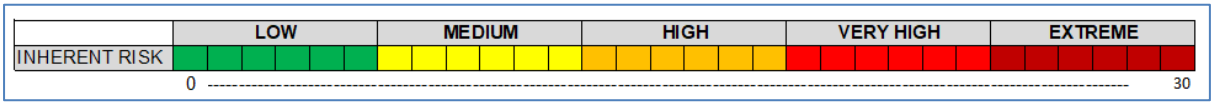


Figure 9: Linear matrix showing impact, likelihood and velocity (Adapted from Quan and Chiang (2017))

2.5.1 *Impact or Consequence*

The risk impact can be described as the potential loss that the organisation faces if the risk materialises. This includes loss in revenue or unforeseen costs. Furthermore, and less quantifiable, is reputational damage which is especially important to large organisations such as banks.

According to the International Organization for Standardization (2009, p. 15), impact or consequence refers to the “outcome of an event affecting objectives. An event can lead to a range of consequences, a consequence can be certain or uncertain and can have positive or negative effects on objectives; consequences can be expressed qualitatively or quantitatively and initial consequences can escalate through knock-on effects”.

2.5.2 *Likelihood or Probability*

Likelihood of risk is associated with the probability of risk materialising. Generally, this gets determined in a qualitative context on a scale from unlikely to almost certain. The product between impact and likelihood is the inherent risk that the organisation faces.

According to the International Organization for Standardization (2009, p. 15), “in risk management terminology, the word “likelihood” is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically such as a probability or a frequency”.

2.5.3 *Velocity or Speed of onset*

Traditional risk models used a typical two-dimensional model where impact and likelihood were the determining factors of risk. More recently, new models proposed includes three or even four dimensions to determine the inherent risk in an organisation. The reasoning is that risk often shares similar impacts and likelihood ratings, yet the speed at which they approach the organisation may differ drastically, resulting in an altogether different risk profile that sits outside of the organisation's risk appetite and planes risk scenarios (Quan & Chiang, 2017).

By adding the velocity dimension, you are building in the risk associated with digitalisation and speed of onset. Speed and velocity clearly play a major role in the characteristics of both big data and cyber-security, to name but two. It is for this reason that it should be appropriate to use velocity during the risk assessment phase of your organisation as these are both systemic and strategic towards the banking environment.

2.5.4 *Proposition 1*

There is an increased inherent risk associated with digitalisation in banking, as digitalisation increases the impact, the probability and the velocity at which risks approach the banking industry.

2.6 The readiness of banks to respond to risks as a result of digitalisation (Risk response)

This would therefore also be an indicator of preparedness for changes. To assess this, a few questions need to be answered. First and foremost, are staff members sufficiently skilled and trained to assess these accurately? This question does not just relate to risk management professionals but also to the business as a whole. This means the three lines of defence (3LoD) need to be collectively prepared. The Basel Committee on Banking Supervision (BCBS) (2015, p. 14), states that “a risk governance framework should include well defined organisational responsibilities for risk management, typically referred to as the three lines of defence”.

These include:

i. First line of defence: The business line, i.e. Marketing, Operations, Sales, Product Management, etc;
ii. Second line of defence: An independent risk management function including legal, risk, compliance and fraud management;
iii. Third line of defence: An independent internal audit function (Basel Committee on Banking Supervision (BCBS), 2015, p. 14).

It is important that these functions are all independent of each other. Together they form the basis of a combined risk assurance approach. This also means that each line needs to be prepared for the risk associated with digitalisation.

Further to this, the tertiary education institutions and professional bodies need to ensure that risk management professionals are sufficiently skilled to address the risks brought on by the 4IR and digitalisation.

2.6.1 *Digital skills of the 3LoD in banking*

Digital skills, at least at a basic level is crucial for the management of risk across the organisation. This means that banks, need to ensure that across their 3LoD skills are optimised to address risks associated with digitalisation.

In their recent report, IRMSA (2020) confirmed that the failure to develop, attract and retain talent is one of the top twelve risks facing South Africa today. This means that functions across the 3LoD are under threat. In their report, they went on to highlight specifically the importance that risk management plays in digital transformation and the necessity for risk management skills to incorporate data analytics and quantitative capabilities to better deal with the speed at which risk is approaching organisation and to deal with enhanced dynamic decision making (IRMSA, 2020).

2.6.2 *Tools used to manage risks*

In non-linear and digitally transforming organisations, the need for identifying both negative and positive risks will greatly increase. Complex systems, coupled with

massive amounts of data that needs to be interpreted for signals and trends will require vastly different tools than what is currently being relied upon (IRMSA, 2020).

To ensure that the risks are adequately managed and timeously responded to, staff need access to the necessary tools to manage digital risks. In the absence of this, risks may go unmanaged, unidentified or unmonitored.

According to RSA Security (2019b), the digital risk management process starts by mitigating the risk of a cyber-attack, securing cloud storage, managing third party risk and by effectively managing a distributed workforce.

2.6.3 *Proposition 2*

Banks in South Africa are prepared to respond appropriately to risks that result from digitalisation, as they are sufficiently skilled and have the right tools to perform their duties.

2.7 Conclusion of the Literature Review

To meet the strategic objectives of the bank, digital transformation is an absolute necessity if the banks in South Africa are going to remain competitive. New business models and digital transformation have not only allowed for an increase in competition amongst traditional retail banks, but it has also created a market for new Fintechs to enter. These changes in the market have been brought about by disruptive technologies and the needs of customers changing.

It is important that banks understand the implications of these disruptive technologies and what they mean for their strategic objectives. Failing to properly recognise and assess risk during the digital transformation journey will result in the organisation being pushed out of the market, either through failing to respond to digital risks or as a lack of keeping up with market forces.

Digital skills and a business digitalisation strategy is crucial for creating the foundation of effectively managing digital risk. The risk management function has become increasingly more important during the 4IR, as digitalisation has brought on risks that require the correct level of assessment and response planning.

2.7.1 *Proposition 1*

There is an increased inherent risk associated with digitalisation in banking, as digitalisation increases the impact, the probability and the velocity at which risks approach the banking industry.

2.7.2 *Proposition 2*

Banks in South Africa are prepared to respond appropriately to risks that result from digitalisation, as they are sufficiently skilled and have the right tools to perform their duties.

3 RESEARCH METHODOLOGY

This chapter outlines the research methodology that was employed to test the propositions made in chapter 2. It explains the research approach, design and the instruments that were used for the research data collection. The chapter ends with discussing the transferability and dependability of the research.

3.1 Research approach

The research undertaken was exploratory in nature to probe the 3LoD understanding and exposure towards the emerging threats and appropriate response that digitalisation introduces into banking. This was not only done to understand the perceptions around digitalisation and associated risks but also to determine perceptions around perceived readiness towards responding towards and managing risks. The research, therefore, aimed to obtain new insights and ask new questions (Saunders & Lewis, 2012).

3.2 Research design

The research adopted a mixed method, case study approach. The research was conducted using online questionnaires and face-to-face interviews, with structured and semi-structured questions. This is important as the research intended to gain insight into the individuals' experiences across the 3LoD of banks in South Africa. The figure below illustrates the design of the research as it relates to the propositions.

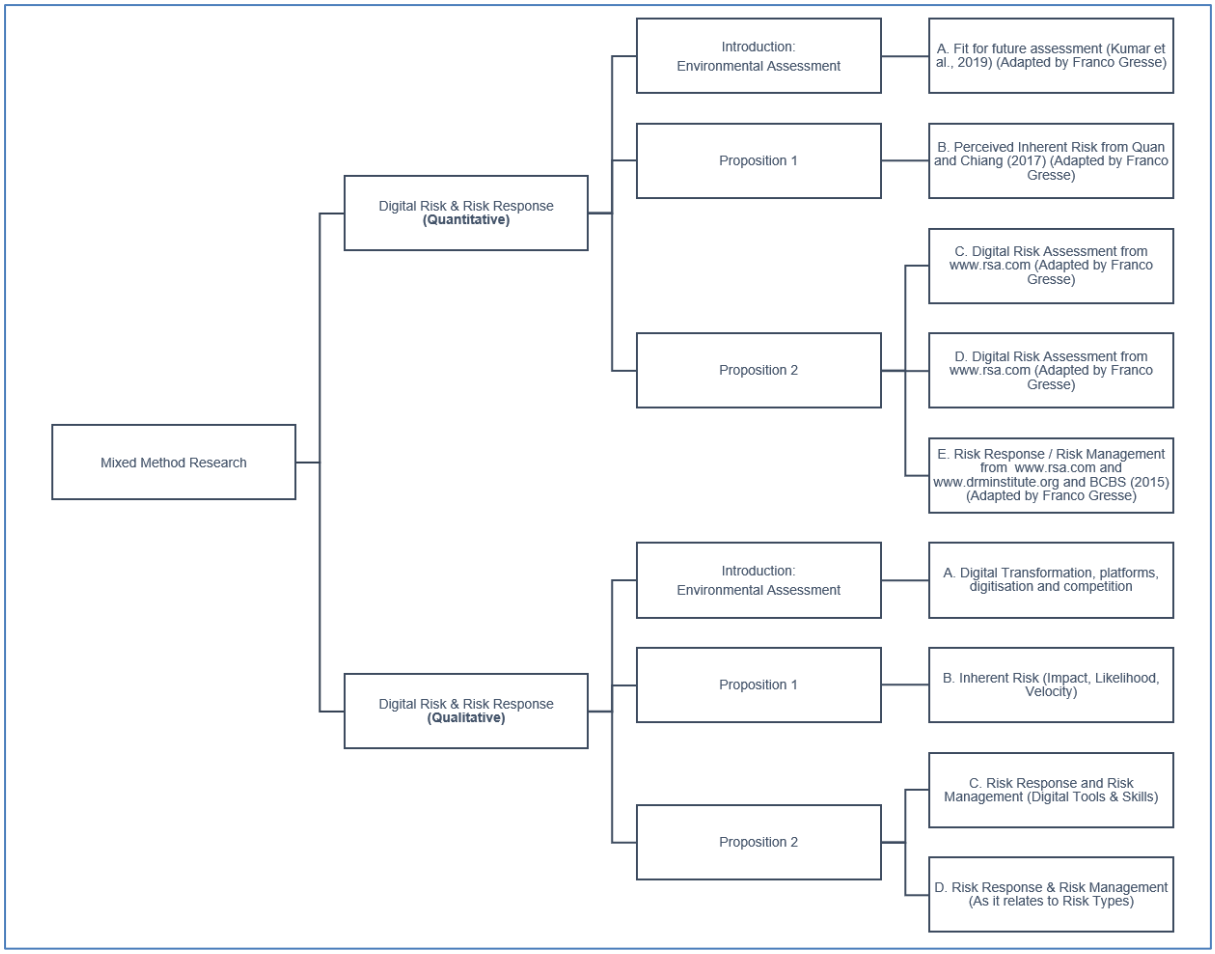


Figure 10: Mixed method research design as it relates to the propositions

3.3 Data collection methods

Surveys were done in the form of web-based questionnaires. These were distributed to the 3LoD across the organisation, with the aim of collecting information from middle to senior managers across the organisation. This is depicted in the figure below. The structured questions were accessed via the web by each respondent, allowing them to capture and record their answers. Using questionnaires allowed for the collection of data from large numbers of respondents, about similar matters or issues (Saunders & Lewis, 2012).

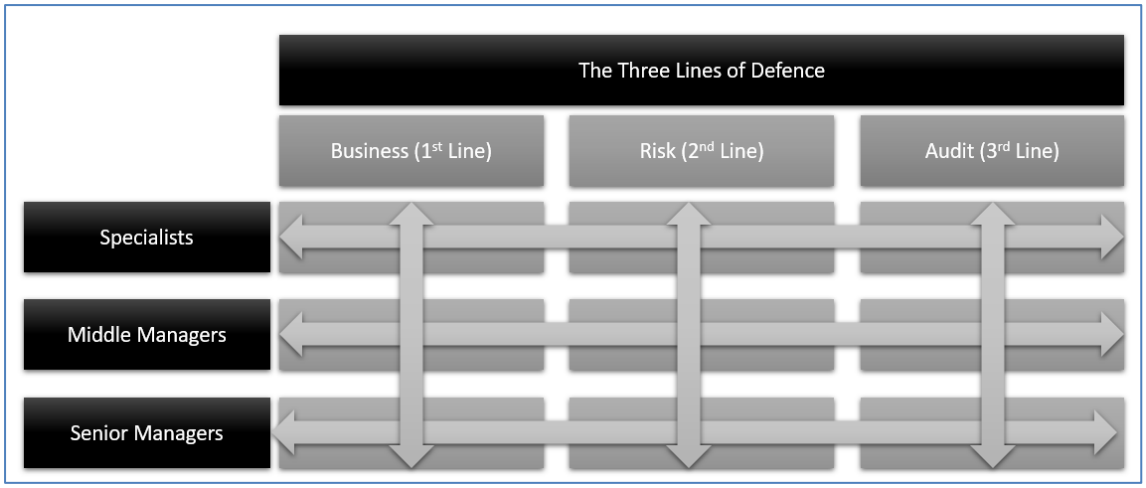


Figure 11: Survey response collection across the 3LoD

To gain deeper, richer insight, qualitative semi-structured interviews were conducted with selected individuals, particularly at senior management level. Saunders and Lewis (2012) recommended that this is suitable in situations where questions can be complicated and require variations to gain further insight.

3.4 Population and sample

The research focused on individuals employed by banks across different 3LoD job functions. These included professional and skilled workers, across age groups, demographics and gender. Interviews were conducted with a select number of senior managers. These included skilled professionals across demographics, age groups and genders. The population is expected to be based mainly in Johannesburg or other major metropolitan areas in South Africa, due to headquarters of the bank being primarily located in these areas.

3.4.1 *Population*

The population of the study is comprised of skilled banking professionals across the 3LoD, including business, risk management and internal audit. These were identified from within a leading retail bank in South Africa.

3.4.2 *Sample and sampling method*

According to the Banks' Annual Report, the group currently employs 48,780 employees. Of these, approximately 5,000 are skilled professional typically employed across the 3LoD. Therefore, the population (N) is equal to 5,000.

Using this population size, at a 90% confidence level and a 10% margin of error, the sample size can be calculated using the following formula (Qualtrics, 2019; SurveyMonkey, 2019):

$$\text{Sample size} = \frac{\frac{z^2 \times p\,(1-p)}{e^2}}{1 + \left(\frac{z^2 \times p\,(1-p)}{e^2 N}\right)}$$

Population size (N): 5,000 **Confidence level (p)**: 90% ($z - score$: 1.65)

Margin of error (e): 0.1 **Sample size (n):** 67

The web-based survey was therefore randomly distributed and at least 67 responses were required across the population. A total of 115 responses were collected, of which 104 was used for the interpretation of the Excel analysis after incomplete responses have been removed from the sample. For the in-depth analysis, a sample size of 113 was used after applying the full information maximum likelihood technique.

For the semi-structured interviews, a sample size of eight from homogeneous populations was required. A total of five participants were interviewed as data saturation was observed, the stage at which additional data collection provided very little novel insights into the research question and objectives (Saunders & Lewis, 2012, p. 158).

3.5 The research instruments

A questionnaire was designed using the Qualtrics tool and the link to access it distributed using electronic communication tools and platforms. The questions were

structured, as a large number of data gets collected from working professionals from a leading retail bank in South Africa. The questionnaire was comprised of open questions and rating questions (Saunders & Lewis, 2012). Furthermore, an interview schedule was used to conduct semi-structured interviews with a select number of senior managers. Unstructured interviews are “a method of data collection in which the participant talks openly and widely about the topic with as little direction from the interviewer as possible. Although there is no predetermined list of questions, the interviewer will have a clear idea of the topics to explore” (Saunders & Lewis, 2012, p. 152).

3.6 Procedure for data collection

Web-based questionnaires were distributed using email and mobile text messaging through professional networks and working groups, that are associated with the bank that is being observed. These included text-based messaging of links, distribution of links via social media platforms and company email distribution lists. The data was collated on Qualtrics for further interpretation. The in-depth analysis required the data to be exported from Qualtrics and to be further analysed using SAS and Microsoft Excel.

Face-to-face meetings were set up to conduct interviews with identified participants. Interview data were collected by means of voice recordings that were transcribed and then used for thematic coding and analysis.

3.7 Data analysis and interpretation

For the quantitative portion of the study, data from the web-based questionnaires were analysed within Qualtrics. Where necessary, an in-depth analysis was performed using SAS and Microsoft Excel for the graphing and explanation of feedback obtained from rating questions.

For the qualitative section of the study, interviews with a select group of senior managers in the organisation were held. Interviews were recorded and transferred into transcripts. The individuals were selected specifically on the job function they fulfil and experience they have, to add richness to the interpretation of the quantitative data

collected through the web-based questionnaires. Individuals were selected using a method called purposive sampling or judgemental sampling.

Purposive sampling is a technique used to select participants in the study due to the nature of the qualities that they possess. It is not done at random and the researcher uses their own judgement to select the individuals due to their background or knowledge of the subject matter (Etikan, Musa, & Alkassim, 2016).

3.7.1 *Factor / Construct Reliability and Validity*

Each sub dimension's items are first assessed for internal reliability using the Cronbach Alpha measure. The correlational analysis (Table 1, at the beginning of the results section below) displays these internal reliability scores in parentheses on the diagonal of the table: Cronbach alphas for all factors and sub-factors in the study are acceptable.

Thereafter, a confirmatory factor analysis (CFA) model is performed on all latent variables, including complexity as the moderator (Hair, Black, Babin, & Anderson, 2009). The CFA is estimated using the full information maximum likelihood model to account for missing data. Assumptions are found to be met, with normalised multivariate kurtosis around 3, no large normalised residuals, and a normal residual pattern (Lee, 2016). Overall, the CFA fits well as seen in Table 1.

Table 1: Confirmatory factor analysis fit statistics

Fit Statistic	'Acceptable' Thresholds (Lee, 2016)	Model fit
Chi-Square	Non significance or significance in smaller samples	92.81(p = .02)
Standardised root mean residual (SRMR)	< .08 desired	.06
Root mean square error approximation (RMSEA)	< .08 desired, < .10 for upper end of confidence interval	.06 (90% CI = .024-.085)
Bentler's comparative fit index (CFI)	> .90 desired	.95
Bentler & Bonnet's Non-normed fit index (NNFI)	> .90 desired	.93

Having assessed the research instrument, the following section discusses the analytical approach taken in the results section.

3.7.2 *Analysis Notes*

This research employs correlational analysis, general linear modelling ANOVAs to assess relationships between demographics and main variables, structural equation path modelling with latent variables (SEM), and moderated mediation (Hair et al., 2009).

The correlational analysis is undertaken using standard Pearson bivariate correlations, for initial indications of variable association.

General linear modelling ANOVA analyses are used to assess relationships between a key categorical demographic variable and the main variables.

In the SEM models, the two-step approach is used, i.e. confirmatory factor analysis as discussed already in the methodology forms the initial measurement model step for construct validation, followed by path models between not only the key latent constructs described in the research hypotheses but also between control variables such as demographics and these variables.

Finally, as seen in Figure 12 below, the fundamental model of the dissertation is partial mediation, involving the relationships Digitalisation → Digital Risk → Response → Impact. In the path models, significant control variables are included on all main variables: only those that remain in some relationship are discussed in the next chapter.

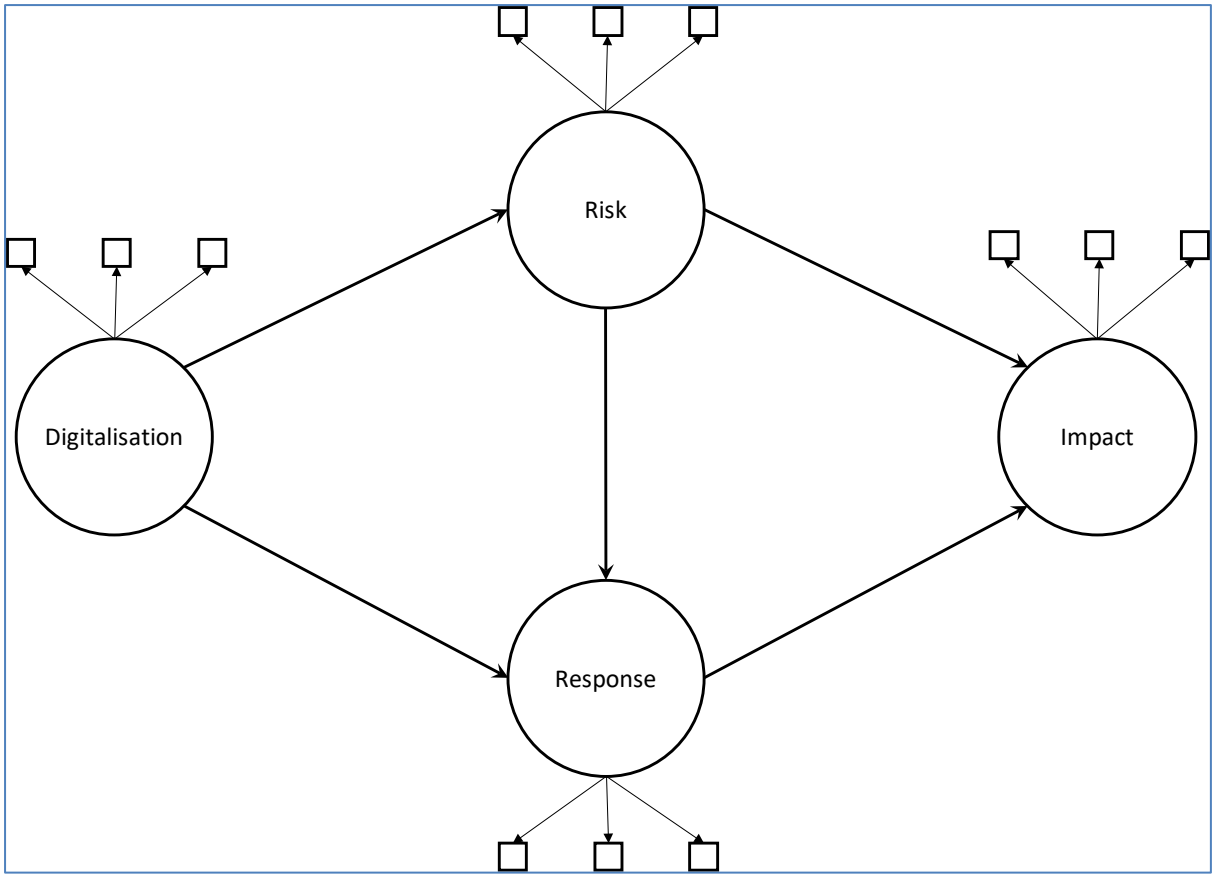


Figure 12: The basic SEM path model (excluding control variables)

Moderated mediation allows the researcher to explore the effect that other variables may have on various mediation paths. The technique of Edwards and Lambert (2007) is used to explore the possible moderation effect of various variables on the core model discussed above. Figure 13 below shows the moderated mediation models to be tested. As seen there, complexity moderates two relationships: those between Digitalisation-Risk-Impact and Risk-Response-Impact.

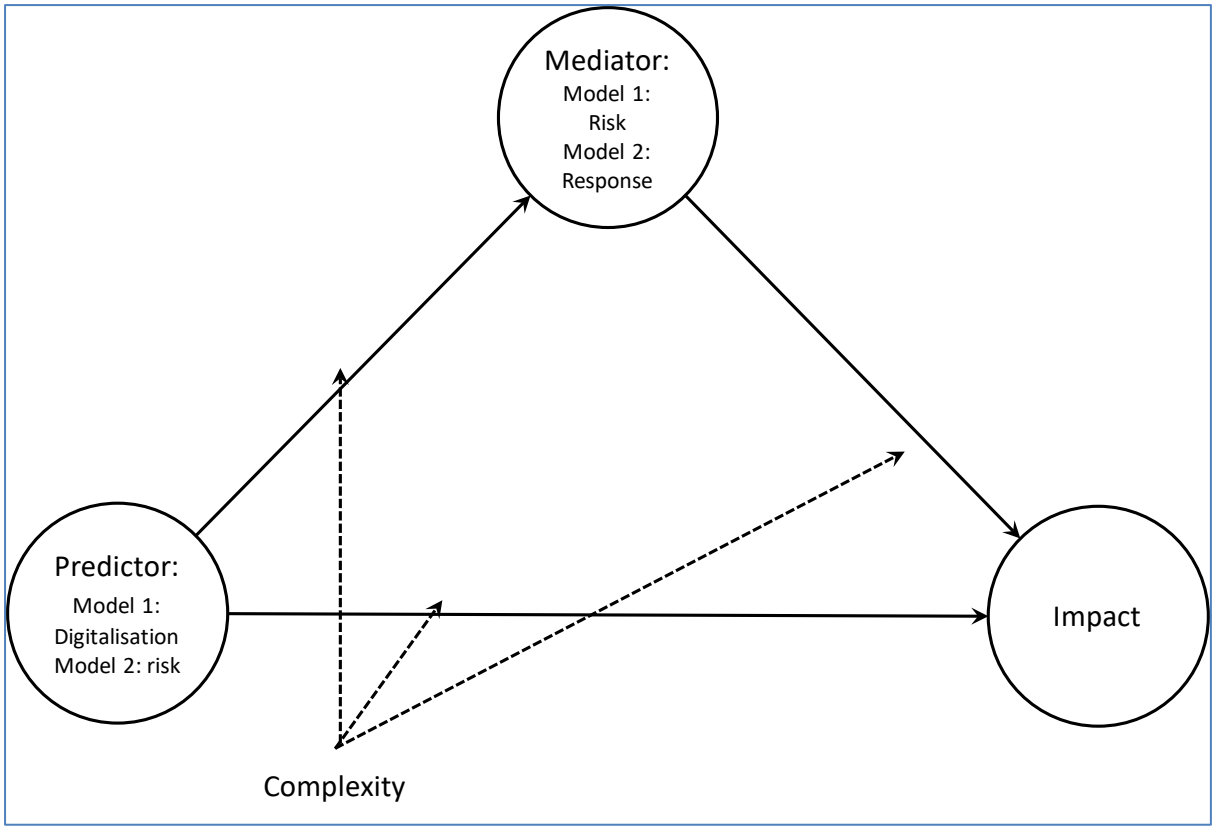


Figure 13: General moderated mediation model

The next chapter of the research report lays out the research results.

3.8 Limitations of the study

i. Human errors and inaccuracy during the completion of the questionnaires.
ii. Based on organisational confidentiality clauses, some questions may not be answered accurately.
iii. Collecting enough responses to provide sufficient insight into the perceptions across the 3LoD of the bank.
iv. Obtaining face-to-face time with senior managers in the organisations.

3.9 Transferability and dependability

Transferability and dependability talk to the degree to which the same results may be obtained if the study was repeated (Morse, 2015). It talks to the trustworthiness of the

findings. The most widely accepted criteria are transferability, credibility, dependability and confirmability (Korstjens & Moser, 2018).

3.9.1 *Transferability*

This will be established through establishing context around the behaviour and experiences as recorded from the respondents. The strategy to achieve this is referred to as thick description (Korstjens & Moser, 2018).

3.9.2 *Credibility*

Credibility is concerned with the element of truth value (Korstjens & Moser, 2018). This will be established in the research through prolonged engagement and data triangulation of responses collected.

3.9.3 *Dependability and confirmability*

The research steps will be transparently reported. This will be displayed through the presentation of an audit trail (Korstjens & Moser, 2018).

3.10 Demographic profile of respondents

Though it was not foreseen that the demographic profile of the participants would influence the results in a meaningful way, some high-level demographic information from the participants were collected for the quantitative portion of the study. This included:

i. Gender.
ii. Age range.
iii. Employment status.
iv. Job function.
v. Period of employment in that job function.
vi. Academic qualifications.
vii. Current field of studies.

For the qualitative portion of the study, no demographic information was obtained as participants were selected based on job role and function the in-depth richness they would add to the quantitative data.

3.11 Ethical considerations

Respondents received a clear and transparent outline of the scope, purpose and outcomes of the research. The information that was collected and its classification and purpose was clearly stated, along with the assurance that consent was received, and anonymity and confidentiality would be maintained.

The research was carried out in a manner that protected the identity of the organisation to whom the participant belongs to. Organisations, participants or any individuals will not be identifiable.

4 PRESENTATION OF RESULTS / FINDINGS

4.1 Introduction

In the preceding chapter, the methodology and the methods used for collecting and analysing the data was discussed. The chapter presents the results from the data collected, using a mixed-method approach. The quantitative data and the resultant findings are first presented, followed by the qualitative findings.

4.2 Quantitative Data

4.2.1 *Introduction*

This section of the chapter looks at the quantitative data that has been obtained through the online questionnaires.

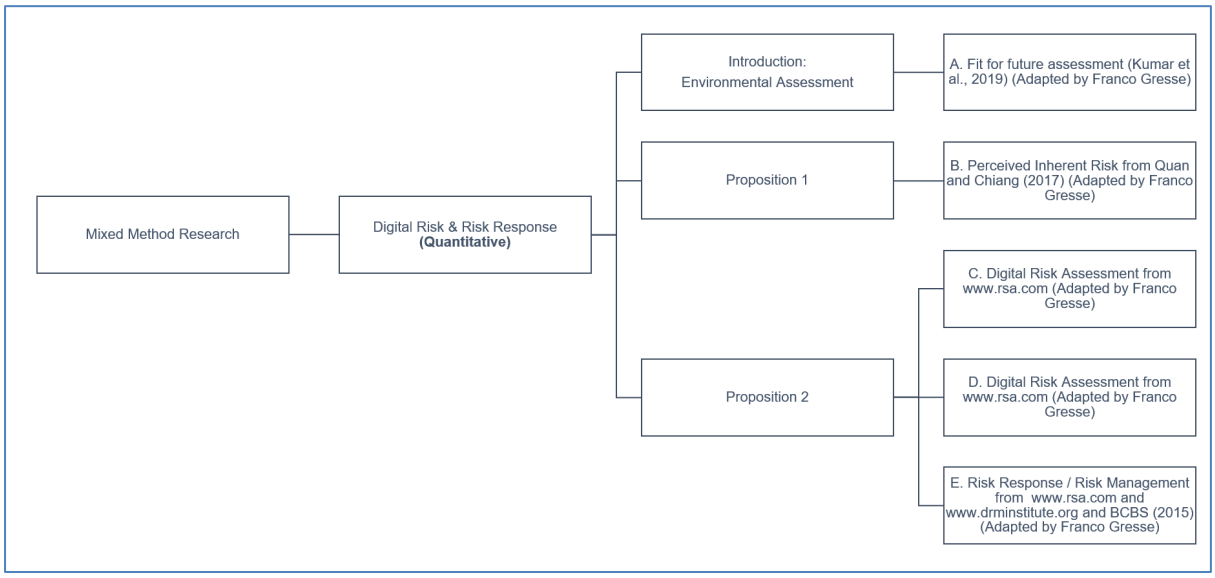


Figure 14: Quantitative Data Collection and Presentation

4.2.2 *Demographics*

4.2.2.1 *Gender*

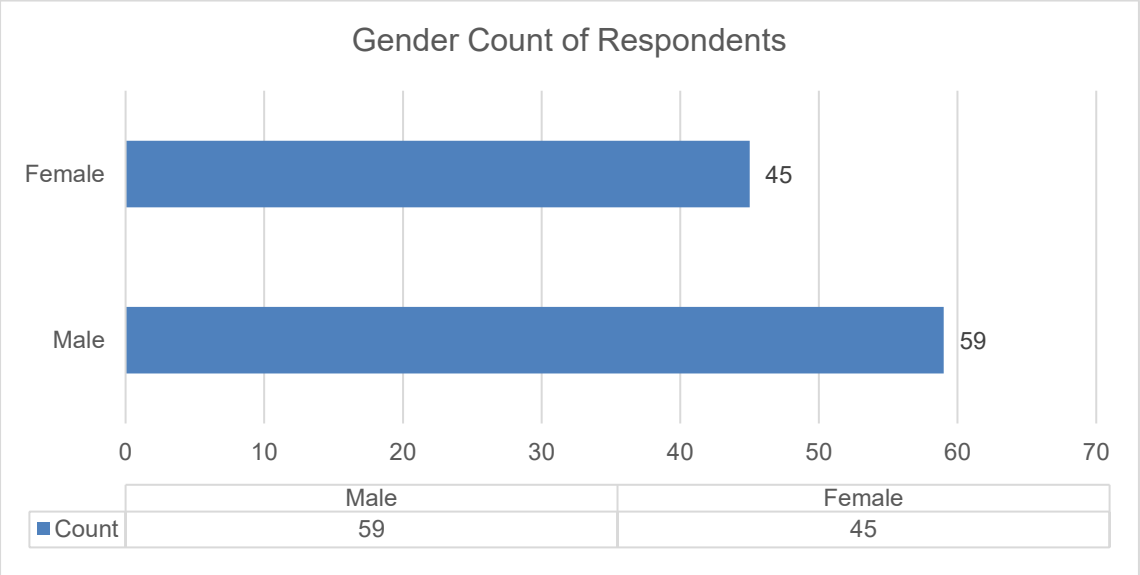


Figure 15: Gender Profile of Respondents (n = 104)

The clustered bar chart shows the comparative view of the number of respondents based on their gender. The graph indicates that out of 104 observed respondents, 57% were male and 43% female.

4.2.2.2 *Age Range*

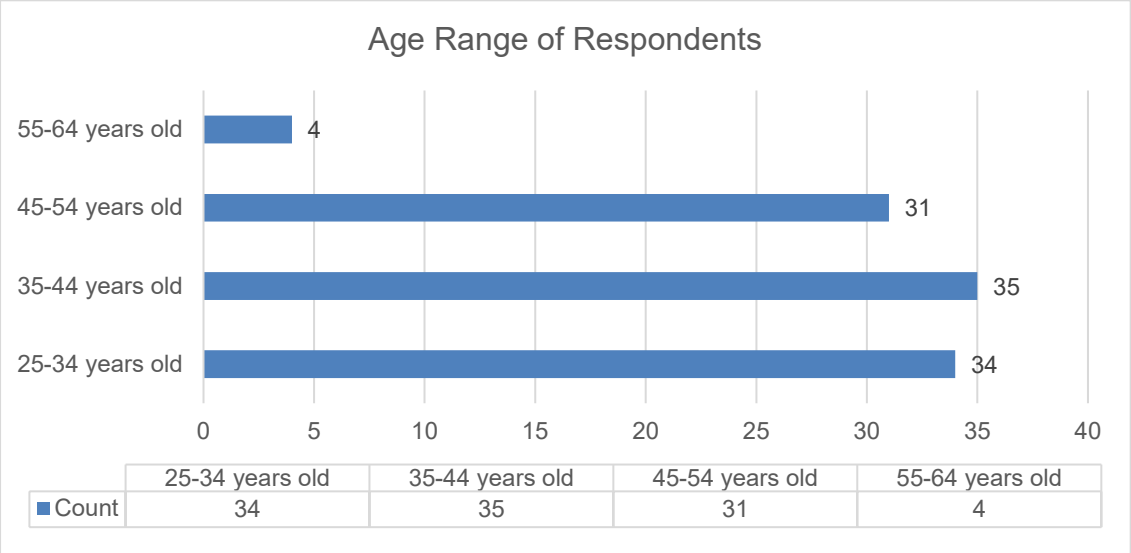


Figure 16: Age Range of Respondents (n = 104)

The clustered bar chart shows the comparative view of the number of respondents based on their age groups. The first three categories are relatively even split with 33% of respondents identifying with the first age group of 25 to 34 years. Followed by 33% of respondents in the second age group of 35 to 44 years and 30% in the age group 45 to 54 years. The last category made up 4% of the total respondents in the 55 to 64 year age group. None of the respondents identified with the age groups 18 to 24 years or 65 and above.

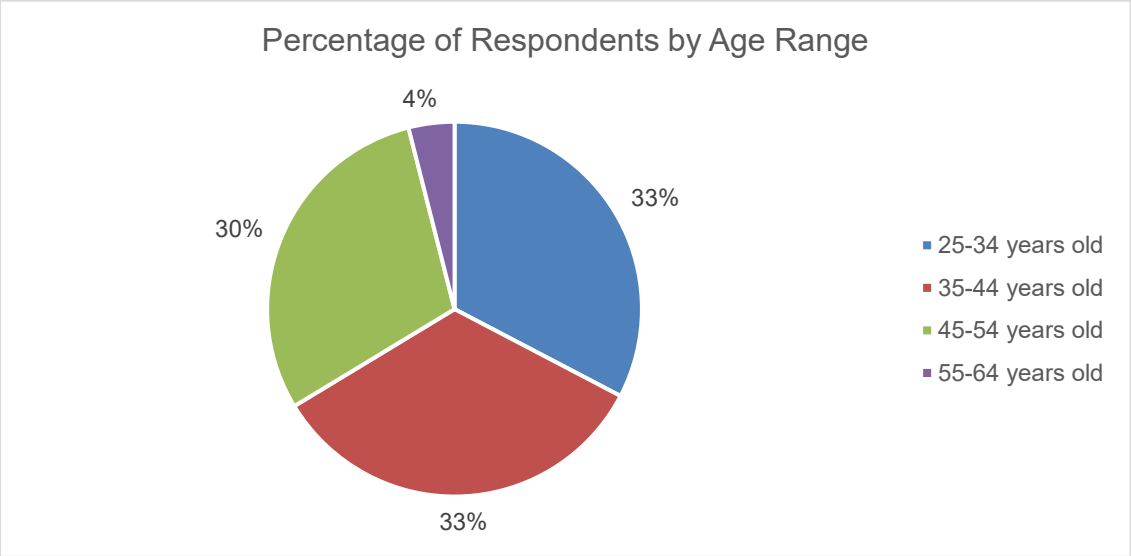


Figure 17: Percentage of Respondents by Age Category (n = 104)

4.2.2.3 *Employment Status*

The figure below indicates that 95 out 104 respondents are permanently employed, with the remainder being temporarily employed or on a contractual basis.

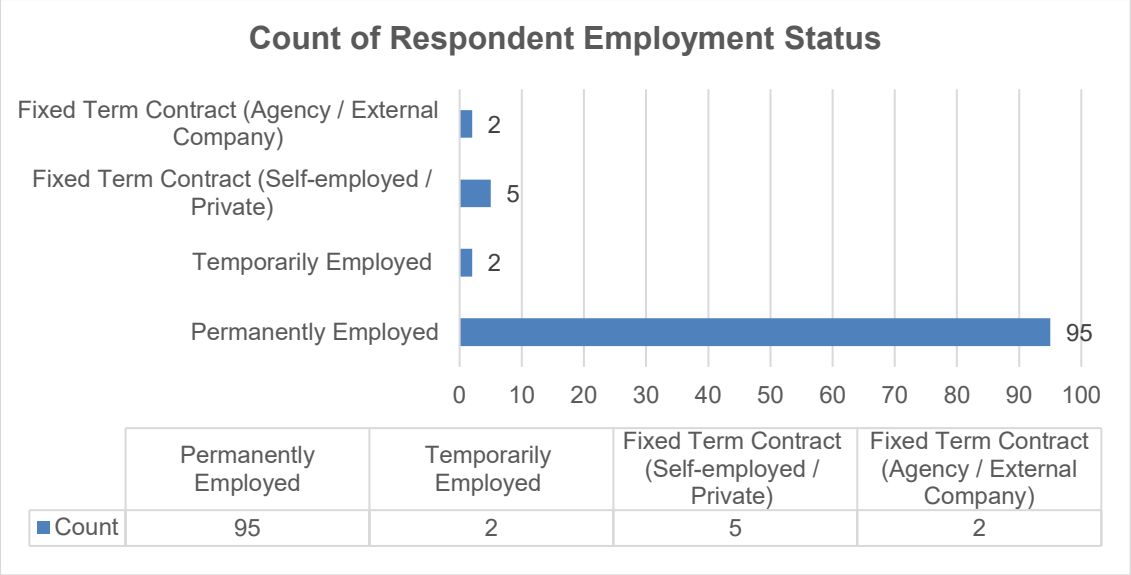


Figure 18: Employment Status of Respondents (n = 104)

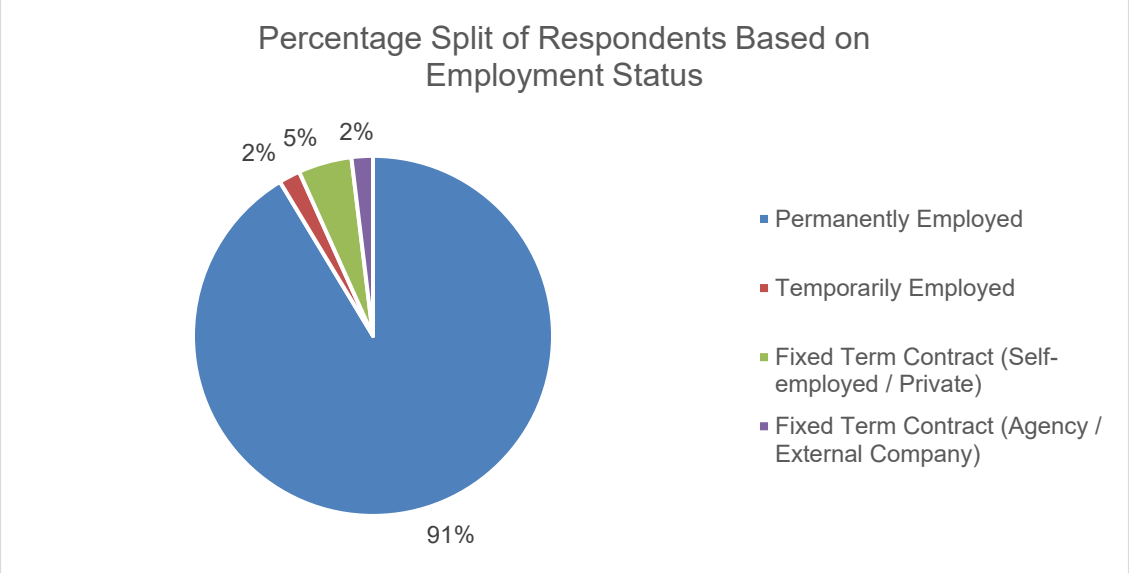


Figure 19: Percentage Split of Respondents Based on

4.2.2.4 *Job Type*

Job Type is assessed as:

1. Business or Business Support (Product, Sales, Operations, Marketing, IT, HR, Finance, etc.),
2. Risk Management (Legal, Risk, Regulatory Risk, Fraud, etc.),
3. Group Internal Audit.

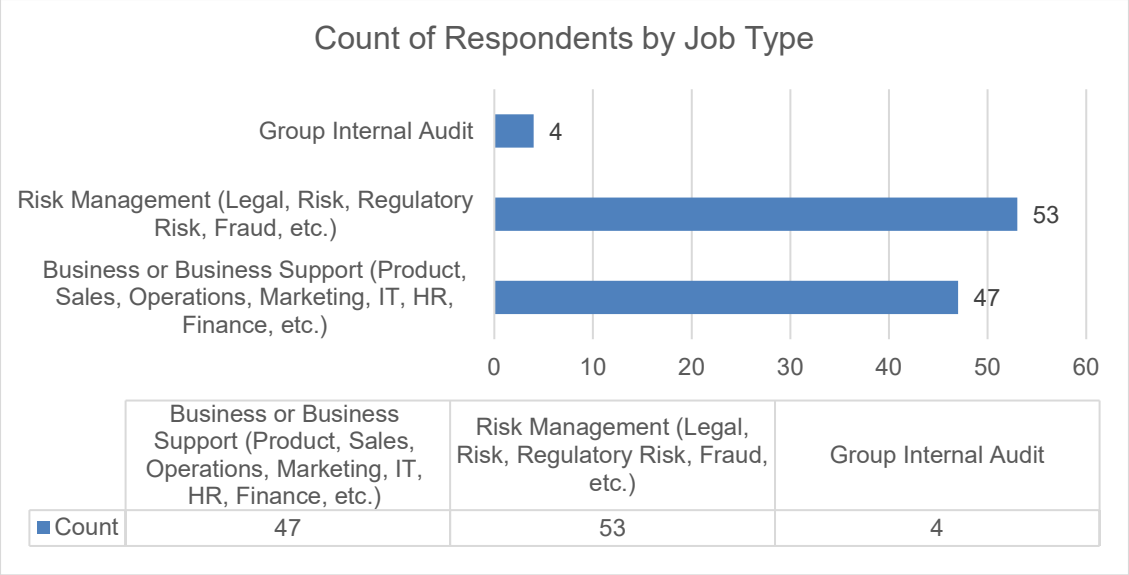


Figure 20: Respondents by Job Type (n = 104)

Because only four responses were solicited from the Group Internal Audit, this category is grouped with Risk Management, and a dummy variable is created where 1 = risk jobs.

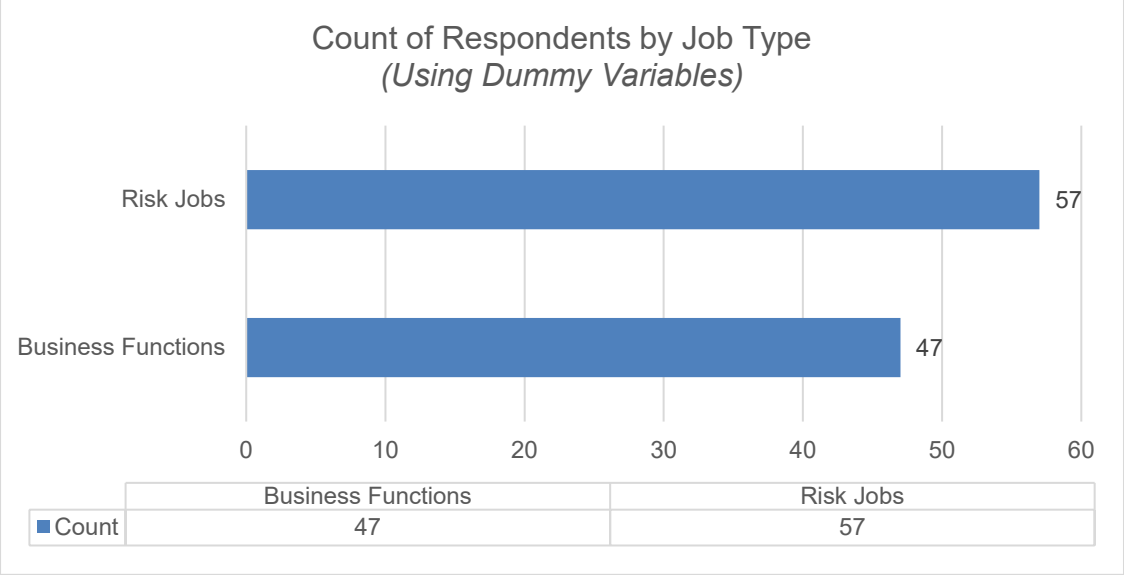


Figure 21: Respondents by Job Type (Using Dummy variables) (n = 104)

4.2.2.5 *Job Role or Hierarchal Level*

Collecting information about the job level at which a person functions in the organisation was considered important, as the perception and understanding of risk

was expected to vary based on the individuals exposure to strategic discussions and policy setting within the organisation.

A method for the handling of missing data in datasets is called Full Information Maximum Likelihood. This technique does not require the missing data to be replaced or imputed, but rather manages the data within the analysis model. Both the Multiple Imputation and Full Information Maximum Likelihood models will yield comparable results (Collins, Schafer, & Kam, 2001).

The hierarchical level is originally measured as an ordinal variable with six ranges being:

1. Specialist & Analyst,
2. Junior Management,
3. Middle Management,
4. Senior Management (non-Exco),
5. Business Exco / Segment Exco (excluding CEO / Segment CxO),
6. Executive (Business CEO / Segment CxO / Organisational Head / CEO).

However, due to uneven distributions of responses, four dummy variables are created:

1. Specialists & Analysts,
2. Lower Management,
3. Upper Management,
4. Executive.

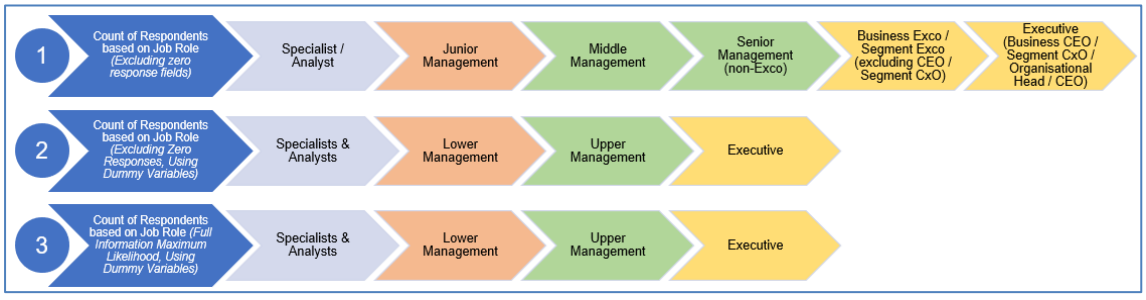


Figure 22: Logical steps of applying dummy variables and applying the Full Information Maximum Likelihood technique

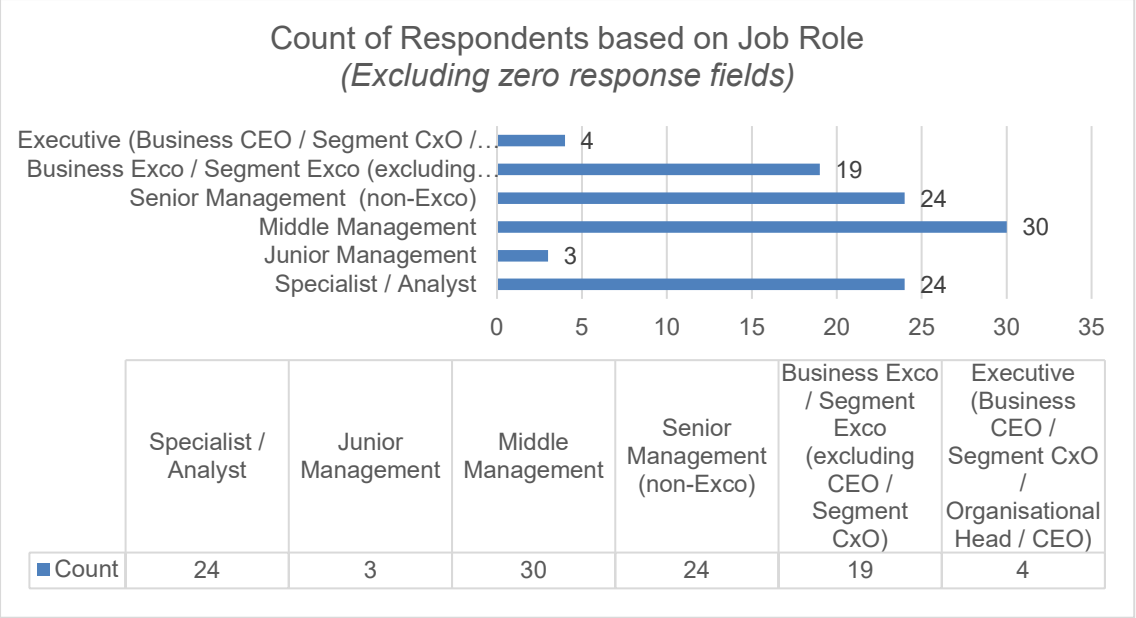


Figure 23: Count of Respondents based on Job Role (Excluding zero response fields) (n = 104)

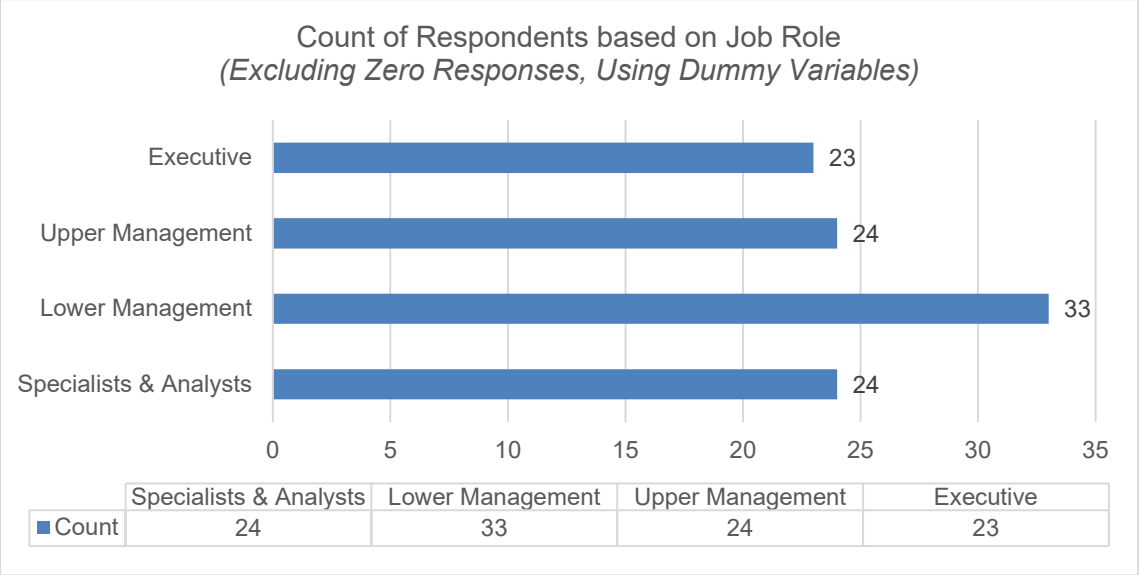


Figure 24: Count of Respondents based on Job Role (Excluding Zero Responses, Using Dummy Variables) (n = 104)

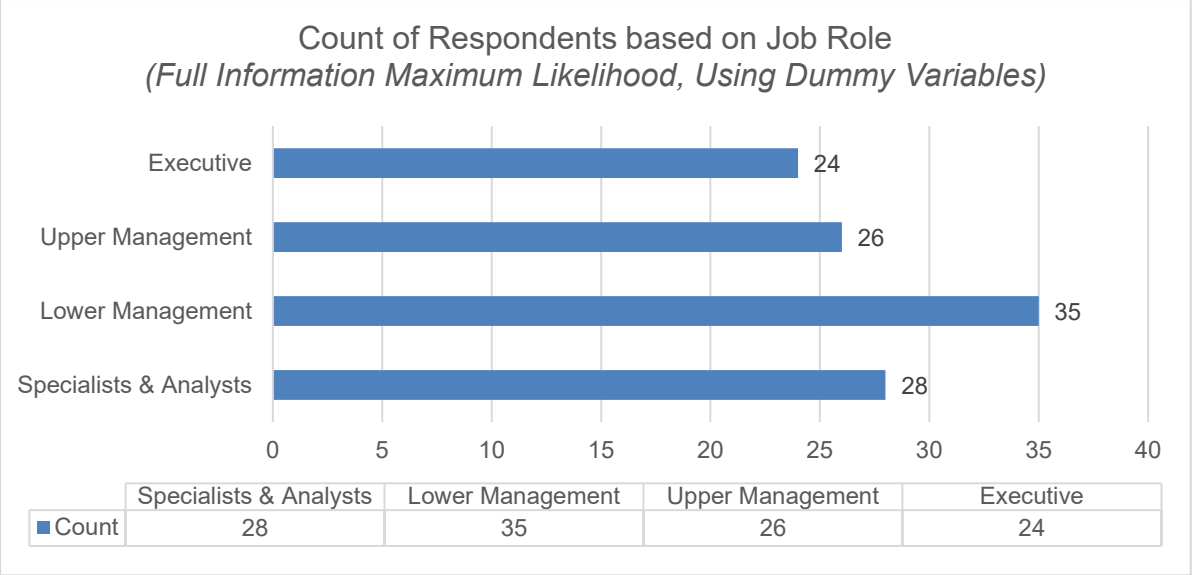


Figure 25: Count of Respondents based on Job Role (Full Information Maximum Likelihood, Using Dummy Variables) (n = 113)

4.2.2.6 *Tenure*

Tenure is reflected as an ordinal variable with ranges from less than three to more than ten years. These ranges include:

1. < 3 years,
2. 3 - 5 years,
3. 5 - 7 years,
4. 7 - 10 years,
5. > 10 years.

Given the number of ranges, this is entered into models as an ordinal variable.

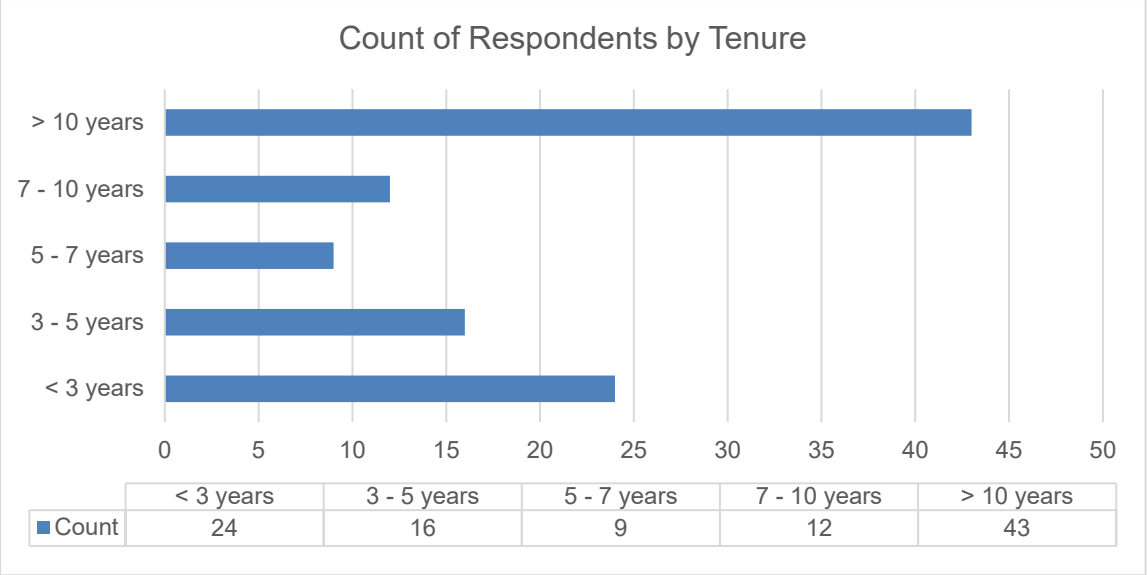


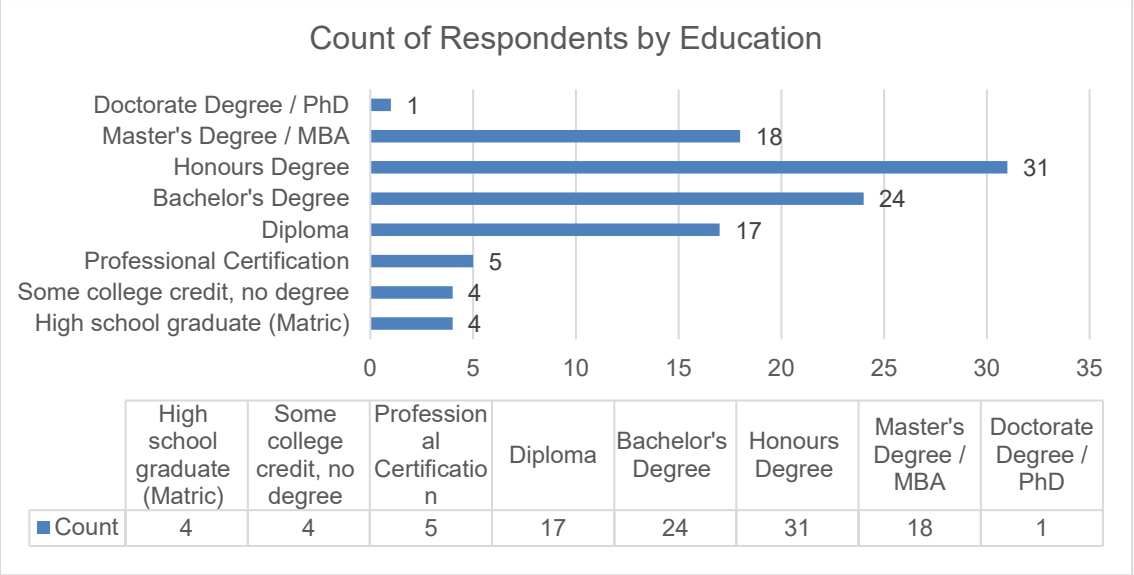
Figure 26: Tenure of Respondents (n = 104)

4.2.2.7 *Education*

Education was measured in ordinal ranges including:

6. High school graduate (Matric),
7. Some college credit, no degree,
8. Professional Certification,
9. Diploma,
10. Bachelor's Degree,
11. Honours Degree,
12. Master's Degree / MBA.
13. Doctorate Degree / PhD.

Given the number of ranges, this is entered into models as an ordinal variable.



	High school graduate (Matric)	Some college credit, no degree	Professional Certification	Diploma	Bachelor's Degree	Honours Degree	Master's Degree / MBA	Doctorate Degree / PhD
Count	4	4	5	17	24	31	18	1

Figure 27: Education Profile of Respondents (n - 104)

4.2.3 *Fit for Future Assessment*

The figure below depicts the recorded responses and respondents were asked to rate each question or category according to their perception of it relative to the organisation's competitors.

At the bottom end of the scale, Disadvantaged would have been selected and at the top end, Industry leadership. The respondents mostly indicated that the organisation is either growing in its maturity or an industry leader as when compared to the rest of the market, with the exception of the category of whether or not risk tools are digitised. Here the respondents rate the organisation the lowest indicating middle of the with 49 responses.

The scale there, in escalating order is:

1. Disadvantaged
2. Experimental
3. Middle of the pack
4. Growing maturity
5. Industry leadership

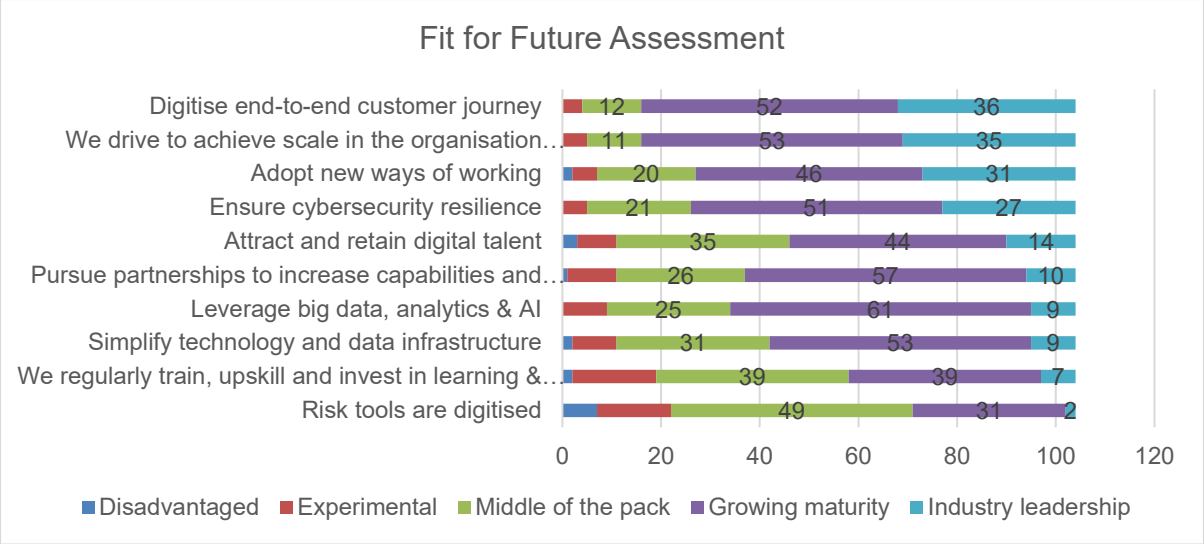


Figure 28: Fit for Future Assessment (n = 104) (Adapted from Kumar et al. (2019))

4.2.4 *Perceived Inherent Risk*

The figure below displays the results from the respondents as it relates to their perception of digital risk when posed with the following three statements, i.e. Digital transformation will result in:

- An increase in risk impact;
- A greater probability the risk will materialise;
- An increase in the speed at which risk approaches the bank.

The respondents indicated that velocity would be the category mostly influencing the inherent risk associated by digital transformation. 43% indicated that they strongly agree followed by a further 33% who somewhat agreed.

The second highest number of respondents felt that digitalisation would shift the risk associated with impact the mostly with 44% indicating that they somewhat agree followed by 38% who strongly agreed.

Finally, respondents indicated that digital transformation would influence the probability of a risk occurring with 33% indicating that they somewhat agree followed by 20% who strongly agreed.

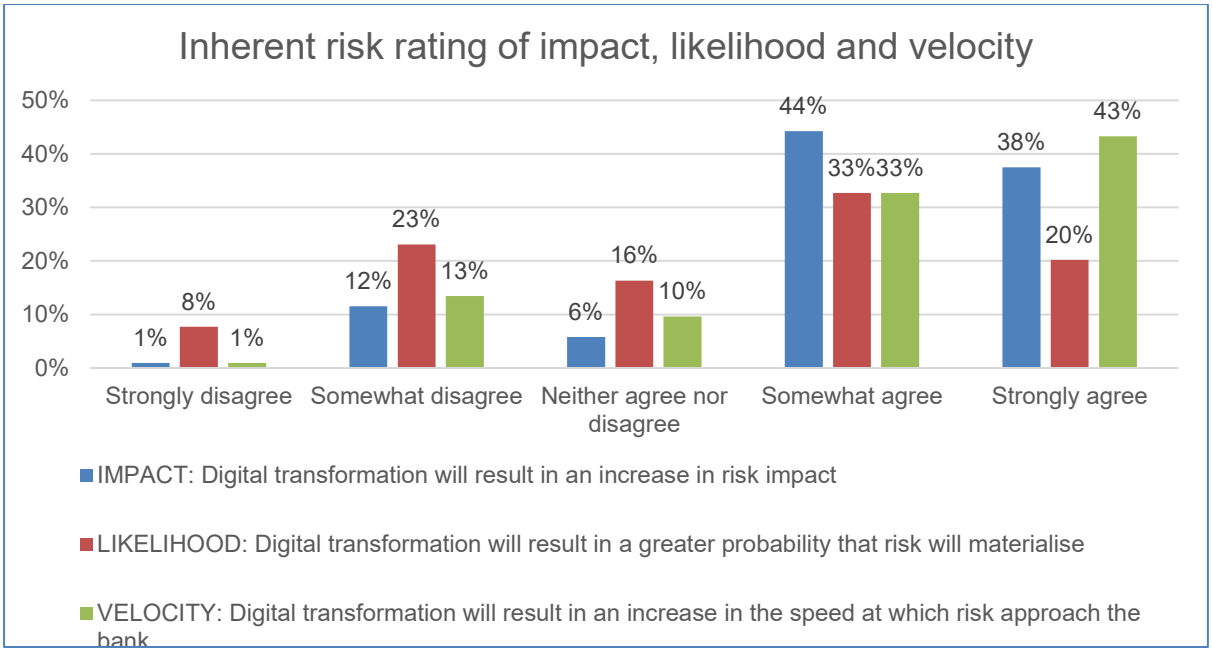


Figure 29: Inherent risk rating of impact, likelihood and velocity

The figure below indicates the 5x5 risk matrix which produces a risk heatmap when the formula of Impact x Likelihood gets applied to each of the responses collected. The responses that were collected as depicted in the previous figure, have then been used to equate it to the risk methodology to calculate the inherent risk, i.e. A selection of Strongly Agree would correlate to a response of Catastrophic (Impact) or Almost Certain (Likelihood). Similarly, if a respondent strongly disagreed, the associated Impact and Likelihood variables would equate to Insignificant or Rare respectively.

This allowed the data to be presented on the risk heatmap, ranging from inherent risk ratings from Low, Medium, High, Very High and Extreme. The concentration of risks can be seen to be around the top right hand corner of the matrix, implying very high (32%) and extreme (19%) risk associated with digital transformation, placing over half of the risk responses in the far right of the matrix.

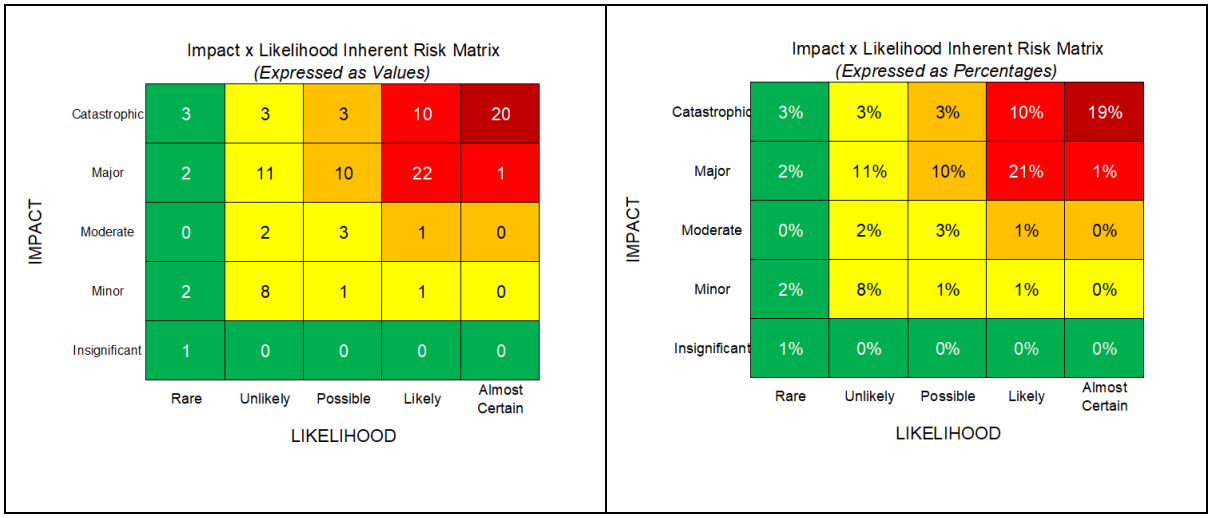


Figure 30: Impact x Likelihood Inherent Risk Matrix (n = 104)

The figure below expressed the same data and values as per the figure above but has been plotted linearly across the risk categories.

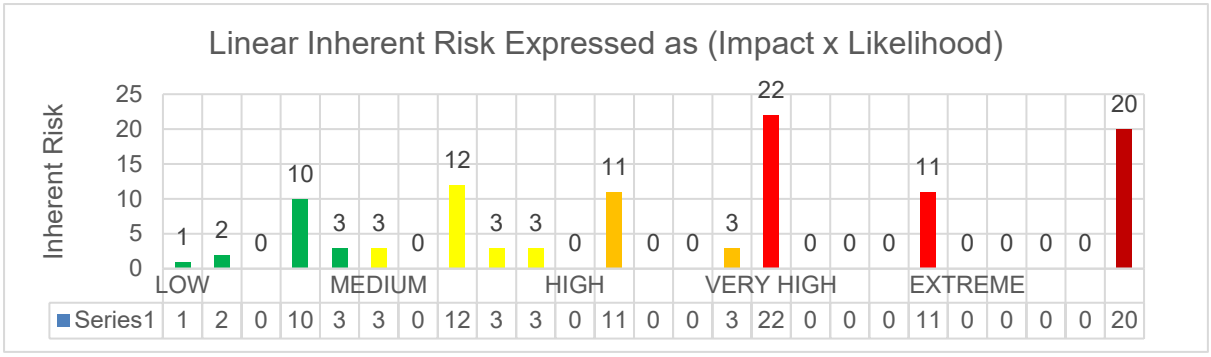


Figure 31: Inherent risk presented in a linear format (Impact x Likelihood)

The figure below now builds on the preceding linear model, by adding the velocity dimension as per the formula, (Impact x Likelihood) + Velocity.

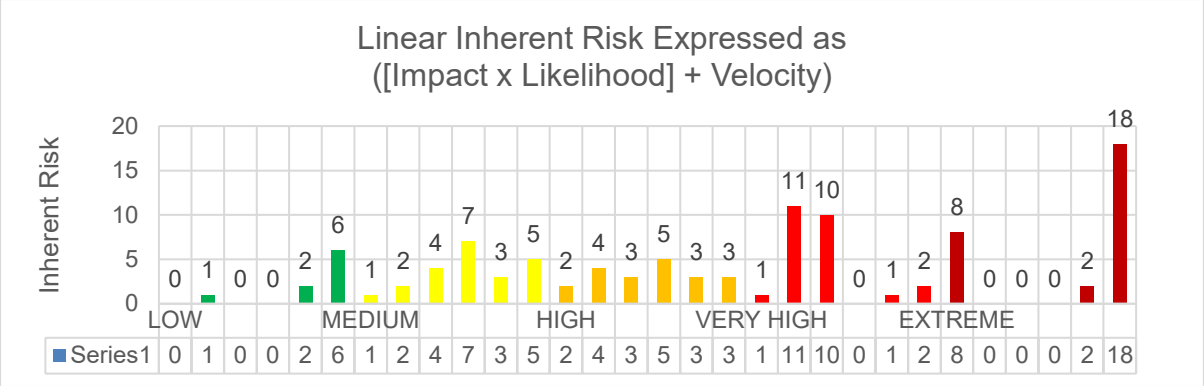


Figure 32: Inherent risk presented in a linear format (Impact x Likelihood + Velocity)

Table 2: Risk profile comparison excluding and including velocity

	(I x L)	(I x L) + V	Diff
LOW	16	9	-7
MEDIUM	21	22	1
HIGH	14	20	6
VERY HIGH	33	25	-8
EXTREME	20	28	8

Table 2 above illustrates the difference between calculating risk two-dimensionally, i.e. Impact multiplied by likelihood (I x L) and comparing it using three dimensions, i.e. Impact multiplied by likelihood and then adding velocity [(I x L) + V] as a third dimension. The difference or shift in the risk profile is illustrated in the third column, showing the effect of adding the third dimension. By including the velocity dimension in the inherent risk calculation, the risk profile shifts the inherent risk factors with nine points, overall resulting in the risks now increasing your medium and high-risk categories with one and six points. Similarly, the very high-risk category shift with eight points being absorbed now in the extreme category. This means that companies, especially those who are in the midst of the digital transformation journey may calculate their risk profiles incorrectly if they forego the use of the velocity dimension in their calculations.

The figure below further demonstrates how the inherent risk shifts from the Low category to Medium and High when Velocity gets added to the model and similarly, from Very High to Extreme.

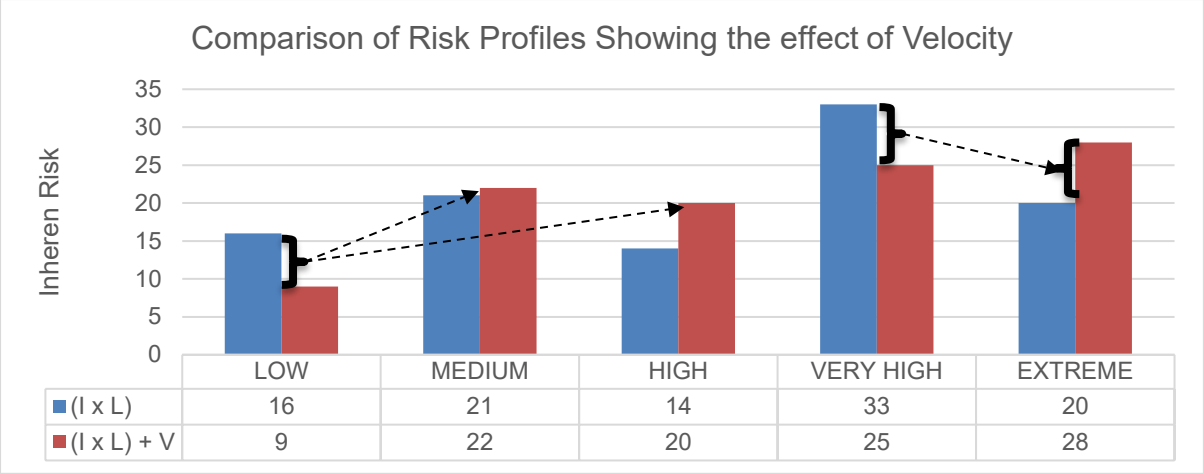


Figure 33: Comparison of Risk Profiles Showing the effect of Velocity

The figure below summarises the risk heatmap in a pie chart, expressed as a percentage where the inherent risk is concentrated. When compared to Figure 30 above, it illustrates that the effect of adding velocity to the model has shifted the Extreme risk category from 19% to 27%.

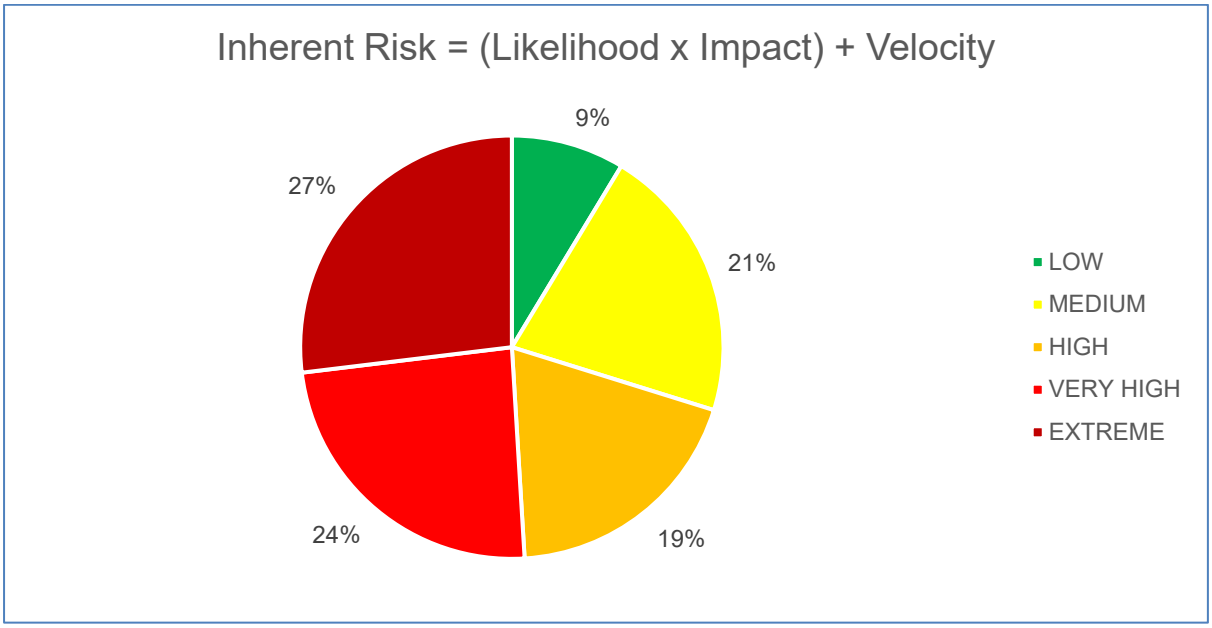


Figure 34: Inherent risk spread across the organisation as a result of digitalisation

4.2.5 *Digital Risk Assessment*

4.2.5.1 *Risk Index*

The responses collected below explains the complexity, third-party dependency and size of the organisation relative to the industry. The greater the size, complexity or third-party dependency, the greater the organisations' inherent risk relative to the industry. The risk index illustrates that a high number of respondents indicated that the organisation is large and rated it highly in terms of complexity.

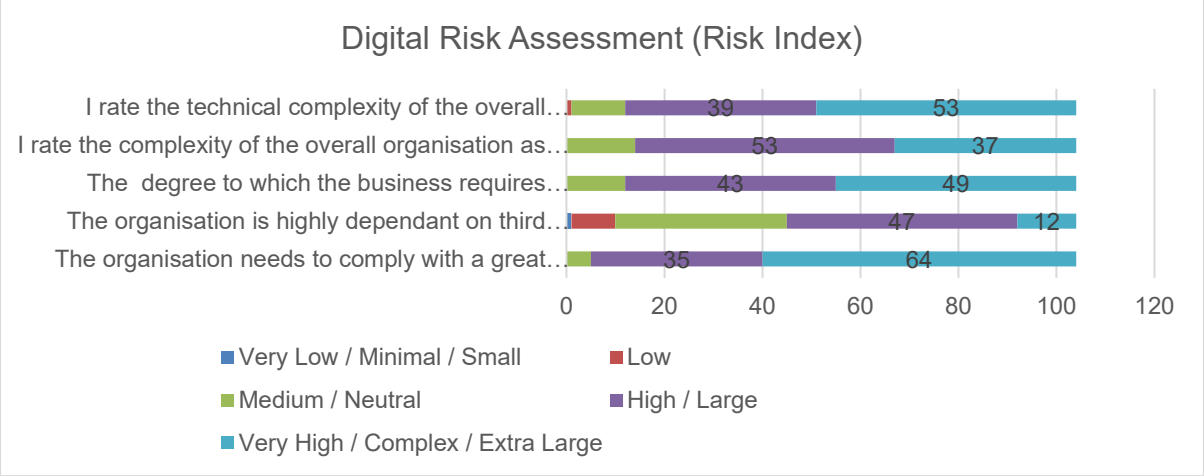


Figure 35: Risk Index in Digital Risk Assessment (Adapted from RSA Security (2019b))

4.2.5.2 *Risk Profile*

The data collected and displayed in the figure below addresses the perception that people have of risk as it relates to the increased inherent risk that digitalisation poses for the business. The table indicates that though there is a perception that risk has increased with the introduction of digitalisation, there is also a perception that the benefits of digitalisation outweighs the risk. Similarly, the majority of respondents the organisation will face serious disruption and threats over the next three years as well as sharing the perception that the risk of a cyberattack or data breach has increased over the past three years.

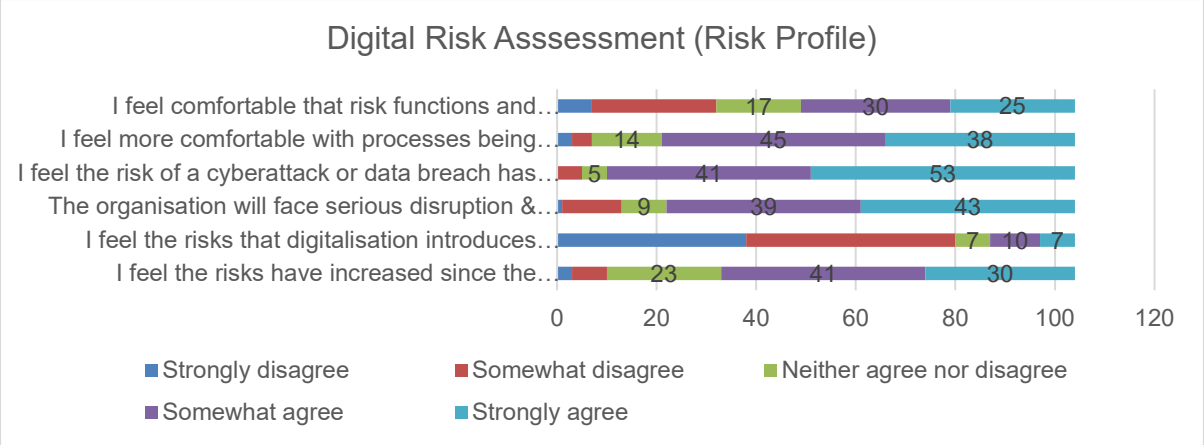


Figure 36: Risk Profile in Digital Risk Assessment (Adapted from RSA Security (2019b))

4.2.6 *Risk Response and Risk Management*

Risk response is crucial to the management of the inherent risk down to acceptable levels. The information collected from the respondents and displayed in the table below illustrates a confidence towards the organisation being positively geared with sufficient controls to manage the inherent risk associated with digitalisation. Perhaps the weakest response observed is linked to the automation of risk processes which may point to a control deficiency in the current environment.

Figure 37: Risk Response and Risk Management (Adapted from Basel Committee on Banking Supervision (BCBS) (2015); RSA Security (2019b); Digital Risk Management Institute (2019))

4.2.7 *Results from the detailed statistical analysis*

As discussed in the methods section, the findings include analyses of bivariate correlations, structural equation path modelling using the latent variables uncovered in the confirmatory factor analysis as discussed in the methods section, and moderated mediation analysis.

4.2.7.1 *Correlational Analysis*

Table 3 below shows the correlations of the variables, which also includes the latent construct Cronbach alphas on the diagonal.

As can be seen in Table 3, digitalisation is significantly related to perceptions of risk ($r = .26$, $p < .01$) and organisational responses ($r = .88$, $p < .01$), but not significantly to perceptions of complexity or impact. Risk is related significantly to perceptions of impact ($r = .70$, $p < .01$), but not to complexity or response. Complexity is significantly associated with perceptions of risk impact (.36, $p < .01$). These results are being discussed in the next chapter. Technically, however, these results seemingly although tentatively support the mediation hypotheses for risk, since digitalisation is associated with risk and responses but not to impact directly, whereas risk is associated with impact.

With respect to associations between demographics and the main variables, few of the results exceed the substantive level of .20 (Lee, 2016). Being on the executive level is significantly positively associated with perceptions of environmental complexity ($r = .28$, $p < .01$), whereas lower management are less likely to perceive complexity ($r = -.31$, $p < .01$). More educated and upper management individuals are slightly more likely to perceive negative impacts from digitalisation ($r = .22$ and .20 respectively, $p < .05$). Finally, perhaps worth mentioning are modestly negative associations between being female and perceptions of risk ($r = -.19$, $p < .05$), complexity ($r = -.19$, $p < .05$) and impact ($r = -.18$, $p < .10$) from digitalisation, as an overall picture this suggests that men are slightly more negative about digitalisation.

Table 3: Correlations and descriptive statistics for major constructs

	M	SD	1	2	3	4	5	6	7	8	9	10	11	12
1. Digitalisation	3.64	.51	(.87)											
2. Risk	3.83	.75	.26***	(.78)										
3. Complexity	4.33	.44	.14	.03	(.74)									
4. Response	3.85	.35	.88***	.09	-.13	(.80)								
5. Impact	3.56	.52	.09	.70***	.36***	-.06	1.00							
6. Female	.42	.50	-.17*	-.19**	-.19**	-.12	-.18*	1.00						
7. Age	2.99	.88	.08	.14	.07	-.02	.16*	-.11	1.00					
8. Risk job	.51	.50	-.04	-.05	.02	-.04	.00	-.02	.05	1.00				
9. EXCO	.21	.41	-.07	.02	.28***	-.14	.16	-.05	.23**	.07	1.00			
10. Upper management	.23	.42	-.07	.13	.11	-.13	.20**	-.13	.32***	.03	-.28***	1.00		
11. Lower management	.31	.46	-.06	-.05	-.31***	-.01	-.16*	.16*	-.15	.00	-.35***	-.37***	1.00	
12. Tenure	3.24	1.67	.18*	-.05	.03	.13	-.02	-.02	.45***	-.03	.32***	.12	-.07	1.00
13. Education	6.02	1.85	-.14	.00	.09	-.11	.22**	-.11	.10	.10	.21**	.10	-.18*	.09

*Note: *** = p < .01, *** = p < .05, *** = p < .10. Cronbach alphas shown in parentheses on the diagonal.*

The next section reports additional general linear model ANOVAs for the one demographic variable that was analysed in categorial format.

4.2.7.2 *GLM ANOVAs for Hierarchical Level*

Analysis of Variance models (ANOVAs) are appropriate models for relating a non-binary categorical variable to a continuous variable. The notable demographic variable in this regard is hierarchical level, as the dummy variables used in other analyses do not directly compare all levels but rather compare EXCO, Upper Management and Lower Management to lower-level employees only. In this analysis, GLM ANOVAs allow direct comparisons of all levels through multiple comparisons. GLM models all use the other demographic variables as control variables.

Table 4 below shows the results for the ANOVA tests. Digitalisation, response and complexity show significant differences, while risk level and impact do not.

Table 4: LS Means comparisons of main variables across hierarchical levels

	Digitalisation (F = .33**)		**Response (F = 4.87***)**
Specialist / analysts	3.92^{a}	Specialist / Analyst	4.08^{a}
Lower management	3.62^{b}	Lower	3.86^{b}
Upper management	3.51^{b}	Upper	3.74^{b}
EXCO	3.47^{b}	EXCO	3.68^{b}
	Complexity (F = 4.81*)**		
EXCO	4.60^{a}		
Upper Management	4.42^{a,b}		
Specialist / Analyst	4.26^{b,c}		
Lower Management	4.14^{c}		

*Notes: *** = p < .01, ** = p < .05. Levels with the same superscript letter have statistically similar mean levels. Tukey multiple comparisons are employed.*

As seen in Table 4, significant differences exist for digitalisation, response and complexity. For both digitalisation and response, specialists/analysts perceive higher levels than management, with no significant differences between management groups. For complexity, EXCO and Upper management perceive higher and similar levels of complexity, although upper management and specialists and analysts have similar levels. Upper management also perceives significantly more complexity than lower management, who in turn are comparable to specialists/analysts. Although more complex than the other two analyses, in essence, this does suggest that higher management perceive more complexity and can be attributed to the strategic nature of their job roles and functions. The next section discusses the main structural equation model.

4.2.7.3 *Structural Equation Path Model*

As discussed in the methods, structural equation models are used to model paths between the main variables as well as demographics, this provides the major main effects tests for the model. Demographics are included as controls on all main constructs but are left out if they prove non-significant. The data for the model fit the analysis, with variables all having acceptable univariate and multivariate kurtosis and multicollinearity tests showing no concerns. Once again, a full information maximum likelihood model is employed to account for the few observations with some missing data.

The model with insignificant demographics removed fits well, with Chi-Square = 109.39 (90), p = .08, SRMR =.06, RMSEA =.043 (90% CI = .000-.070), CFI = .96, NNFI = .94. This indicates a good fit to the model.

Figure 39 below shows the major results for this analysis.

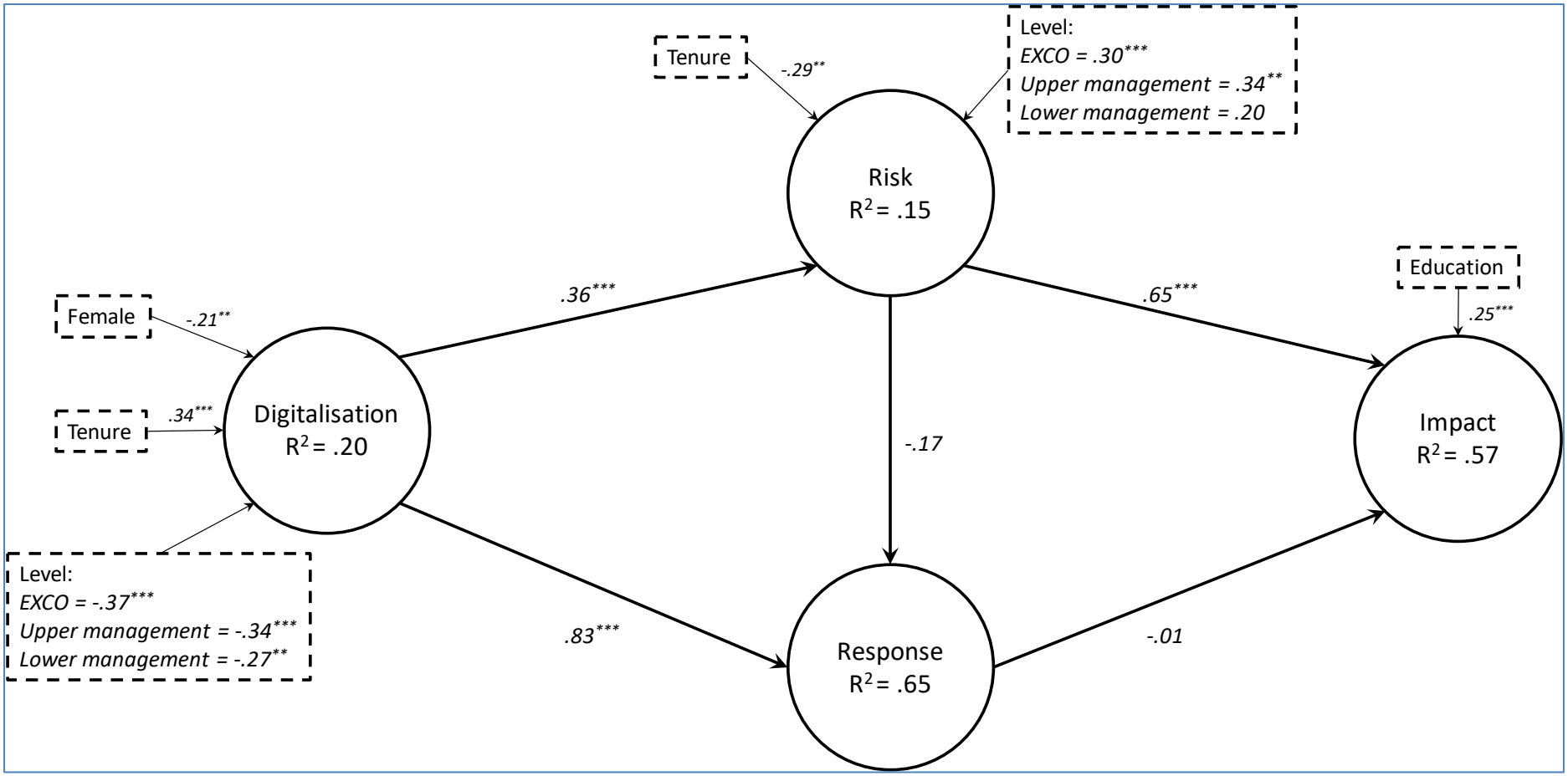


Figure 38: Main Structural Equation Model

*Notes: All paths shown are standardised. *** = p < .01, ** = p < .05.*

As can be seen in Table 5, digitalisation is moderately positively associated with risk (β = .36, p < .01) and very strongly associated with perceptions of response (β = .82, p < .01). Risk is not significantly related to perceptions of adequate responses, but is related to impact (β = .65, p < .01). Responses are not related at all to impact.

In addition to these effects, various demographic control effects can be seen.

The mediation model allows for a decomposition analysis that distinguishes between direct, indirect and total effects, as seen in Table 5 below.

Table 5: Decomposition Table for main SEM Results

	Endogenous Variables			
	Digitalisation	**Risk**	**Response**	**Impact**
Digitalisation				
Direct effect	-	.36***	.82***	-
Indirect effect	-	-	-.06	.22**
Total effect	-	.36***	.77***	.22**
Risk				
Direct effect	-	-	-.17	.65***
Indirect effect	-	-	-	-.01
Total effect	-	-	-.17	.65***
Response				
Direct effect	-	-	-	-.01
Indirect effect	-	-	-	-
Total effect	-	-	-	-.01

*Notes: All paths shown are standardised. *** = p < .01, ** = p < .05, * = p <10.*

As seen in Table 5, the only notable effect that builds on the main direct effect diagram is the indirect effect of digitalisation on impact, which is $\beta = .22$ ($p < .05$). Predominantly because of the perception of increased risk, digitalisation has a modestly positive association with perceived impact.

The results section considers the possible impact of complexity as a moderator on the main mediation model.

4.2.8 *Moderated Mediation Models*

Moderated mediation is used to ascertain whether extraneous variables to the main model may substantially increase or decrease the strength of one of the main model paths. The analytical approach suggested by is employed. In all cases, complexity of the environment is used as the moderator. The MODMED macro in SAS is used to produce analyses, noting that the macro produces unstandardized analysis and therefore shows different path sizes to those in the SEM model.

The first moderated mediation to be examined is that for the Digitalisation-Risk - Impact portion of the main structural model. Figure 40 below displays the results and methodology for this analysis.

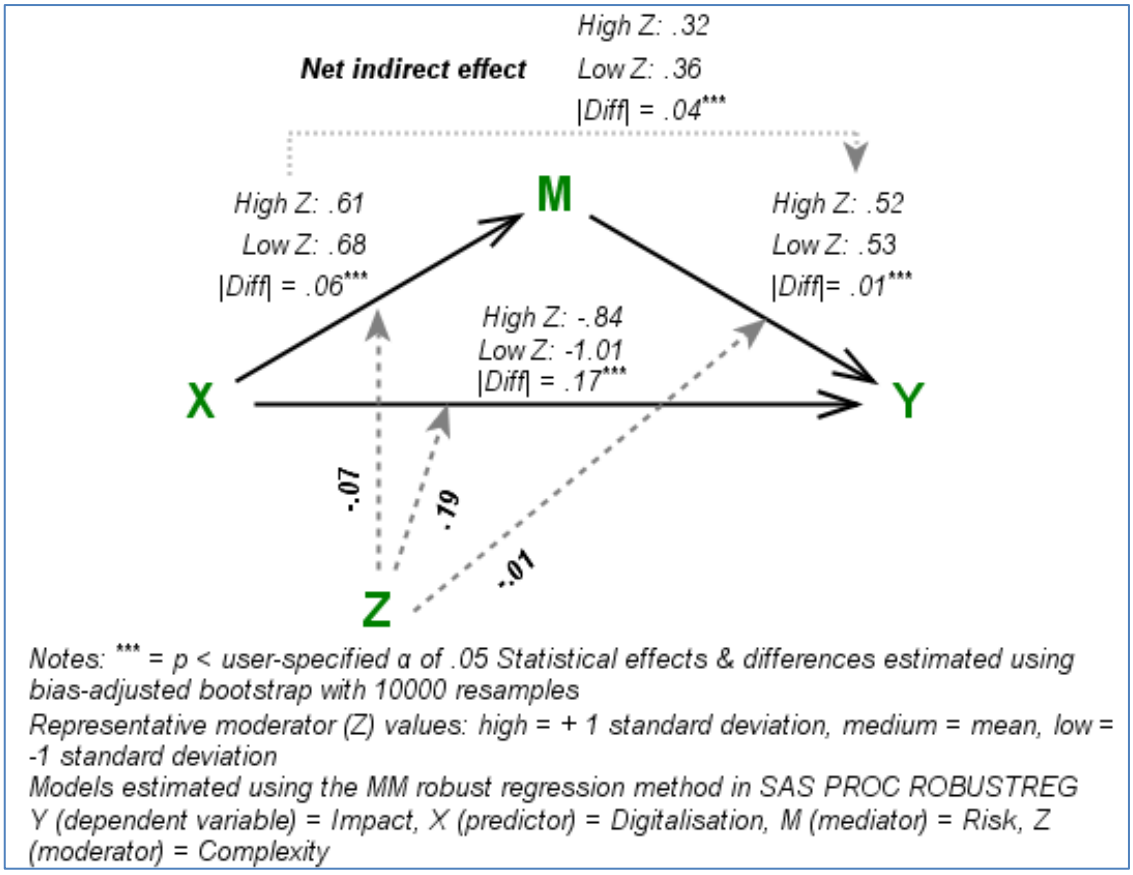


Figure 39: Moderation of complexity on the Digitalisation-Risk-Impact relationships

As can be seen in Figure 40, complexity has the following effects:

- Higher complexity seemingly lowers a direct negative relationship between digitalisation and impact, which would capture the total effect other than the mediation through risk.
- Complexity slightly lowers the positive relationship between digitalisation and risk, which is perhaps opposite to what would be expected.
- Complexity very slightly lowers the positive relationship between risk and impact, although this effect seems so small as to be trivial.

The second moderated mediation to be examined is that for the Risk-Response-Impact portion of the main structural model. Figure 41 below displays the results and methodology for this analysis.

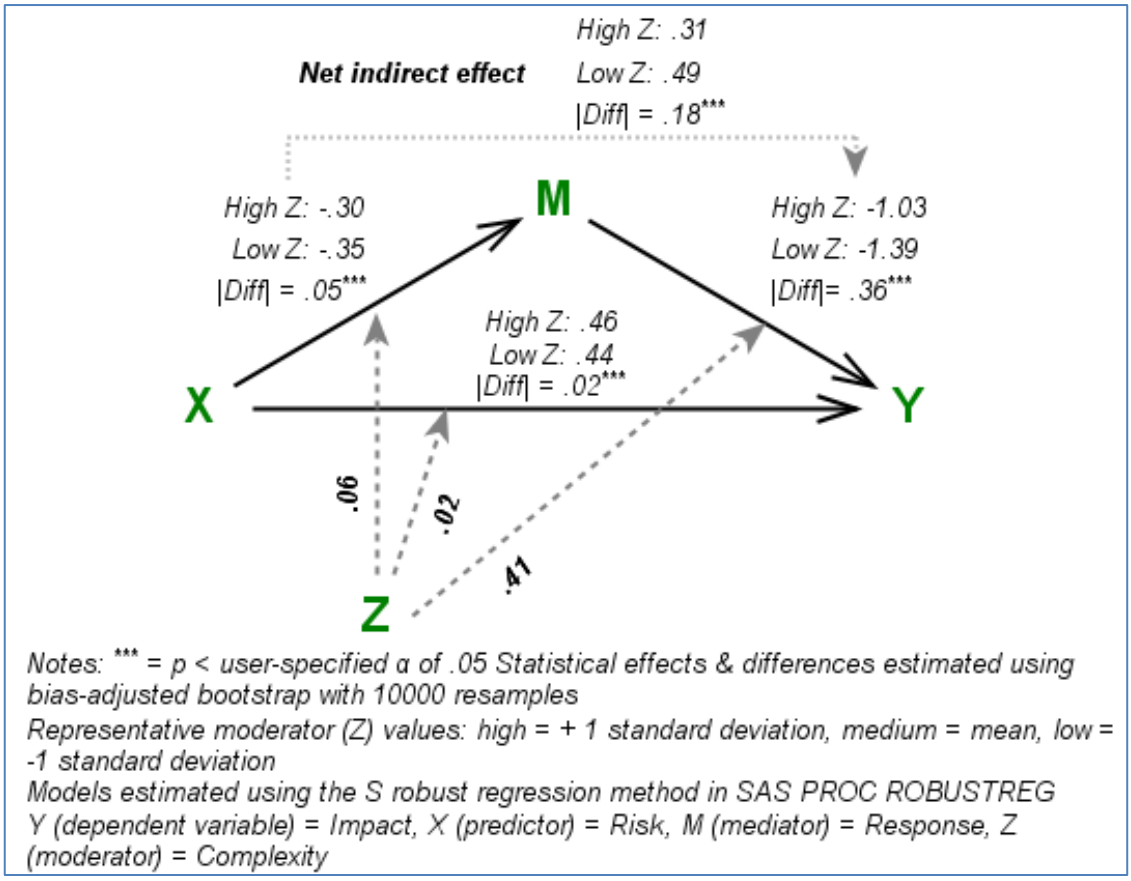


Figure 40: Moderation of complexity on the Risk-Response-Impact relationships

As can be seen in Figure 41, the complexity of the environment moderates all three mediation relationships to some extent:

- Complexity makes the effect of risk on both the response and the impact more positive: in more complex environments, organisations are somewhat more prone to respond to risk with response mechanisms, and the impact of the risk can be more pronounced.
- More complex environments reduce the tiny relationship between the organisation's response and the impact of digitalisation risk.

However, since neither of the response relationships is substantial or significant on their own, this analysis may not be particularly meaningful.

The next chapter discusses these results.

4.3 Qualitative Data

4.3.1 *Introduction*

The following section of this chapter highlights the key themes and concepts that have been collected as part of the qualitative portion of the mixed-method study.

The figure below illustrates how the interviews support the study and show how the interviews have been structured to:

A. Perform an environmental assessment of the bank's digital transformation strategy, including platform thinking and competitive landscape.
B. Understand the inherent risk associated with digitalisation in banking as it relates to Proposition 1.
C. Understand the risk response and risk management strategies that the bank has in place as it relates to digital tools and skills.
D. Understand the bank's risk response and risk management strategies as it relates to different risk types.

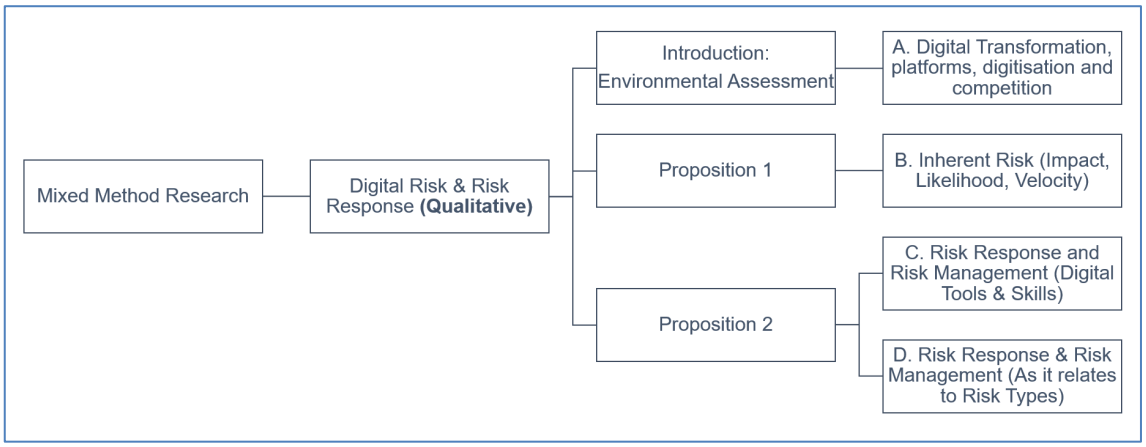


Figure 41: Qualitative Data Collection and Presentation

A total of five interviews were held with senior members of the organisation. These interviews range in duration of between 35 minutes to one hour. The participants had experience and industry knowledge in the following fields:

i. Risk management and engineering.
ii. Legal, compliance and data governance.

iii. Data management, analytics and information management.
iv. Information technology risk management and cybersecurity.
v. Enterprise risk management and legal risk management.

4.3.2 *Section A - Digital Transformation, platforms, digitisation and competition*

In the first section of the interviews, it was necessary to create the foundations of the bank's digital transformation strategy, before we could determine the risk associated with it. It was necessary to understand the bank's foundations as it relates to their digital transformation strategy.

The flow of this section of the questionnaire is diagrammatically depicted below, and the results are presented as part of this chapter.

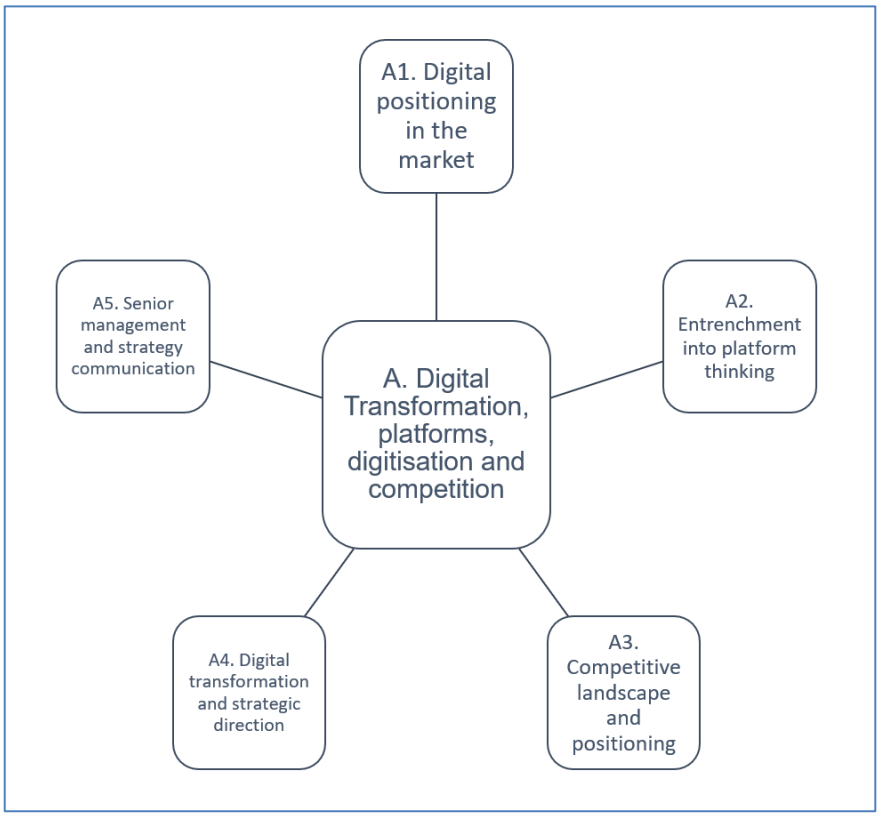


Figure 42: Components that make up the environmental assessment of the interview

4.3.2.1 *A1. Digital positioning in the market*

The interviews, therefore, sought to explore the banks digital positioning in the market relative to traditional competitors as well as new entrants like Fintechs. All of the participants responded positively, in relation to whether the bank is a market leader when compared to its traditional competitors in the market.

> *"Historically, one the bank has been a very innovative bank. And that is evident from the fact that it was the first to launch a range of non-banking services. Internally, one can observe that the bank is introducing different technologies they are looking at improving the way that they actually engage with the customers." (*Participant *1)*

Continuing onwards from the first participant, a strong sense of customer-centricity was also observed to be at the centre of the digital transformation strategy of the bank, further defining their leadership position.

> *"So, so I would say yes, and the reason for that is our approach in putting the customer first and, introducing, let's call it platform functionalities and capabilities that would make life easier for our customers from a banking perspective." (Participant 2)*

Participant 3 continued by adding that data plays an important role in this journey of digital transformation and becoming a market leader.

> *"Yes. I think the key component is the use of data on the forefront of banking." (Participant 3)*

Participant 4 continued by also commenting positively on the banks approach towards platform thinking and embracing elements such as staff mobility and communication.

> *"I think, in terms of taking the lead. Definitely, yes. A lot of this has come around from the whole group strategy of making people, a lot more mobile, bringing a product on platforms that our customers can access on the go. And I think, on the ground and at roots level, this has been something that*

has been well communicated as a strategy and as a way forward to the staff." (Participant 4)

Participant 5 added dimension of cost and operational efficiency in order to remain competitive in the changing landscape.

"So, I think we are a definite leader. I think that other banks have slowly started to realize that, in order to compete effectively and cost-efficiently, that they also need to be on digital channels, and they invested a lot of money in this. Therefore, we're not the only ones in the space, we have very close competition." (Participant 5)

4.3.2.2 ***A2. Entrenchment into platform thinking***

The interviews then aimed to understand how entrenched the bank is in terms of its platform thinking. Almost all of the participants except for one believed that there is a movement towards it, but improvement is required to become fully entrenched.

On the question of whether or not the bank has fully entrenched itself into platform thinking, the respondents had the following to say.

"No, the bank is basically still trying to inculcate that type of culture, to instil that culture into staff. And many staff have not yet bought into the concept or understanding of it." (Participant 1)

The second respondent had the following views.

"So, I would say that platform thinking is really starting to accelerate. However, through my engagements throughout the group, I don't see it in certain areas." (Participant 2)

The third participant had similar views to the previous participant, almost echoing the same sentiment that the thinking is there to a degree, but that it lacks consistency throughout the group. Participant 3 acknowledged the pioneering efforts of some of the business units in the organisation but put forward that there

is still some way to go before platform thinking is entrenched across the organisation.

> *“I don't think entirely my personal view. I think that the platform thinking is there, and I think that the pioneers, are important and that they are leading the way forward. I think where they are struggling a little bit in my view again. There's lots of business units in the bank that operate in silos.” (Participant 3)*

Participant 4 believed that platform thinking was entrenched across the organisation. In turn, Participant 5 took a similar stance to Participant 2 and 3, but instead of looking at it being siloed vertically in the organisation, instead put forward the idea that across the different layers of management, i.e. horizontally there is a greater need for improvement.

> *“I think it's a journey. I think that in the upper levels of the organization there's definitely a high awareness that we have to become a platform bank. I think the challenge lies in terms of taking down that message into middle and lower management, middle management and the structure below middle management, in terms of taking them along that journey and having them apply the minds to move away from the traditional forms of banking to digital platform based bank.” (Participant 5)*

4.3.2.3 ***A3. Competitive landscape and positioning***

The interview explored the competitive landscape in banking and how it has been perceived to change especially with emerging entrants in the form of Fintechs. Across all the participants there was agreement that the competitive landscape has definitely changed, and that Fintechs are playing to their strengths in the agility of infrastructure and regulatory obligations, as to where traditional banks typically are slower to change.

> *“And I also think that the Fintechs are largely unregulated but provide banking wide services. We call them shadow banking, are also very competitive in the space. They don't have the legacy costs that we do*

associated with some of our systems etcetera so they far more agile in the market." (Participant 5)

Participant 4 echoed the agility of the new entrants into the market as a threat to traditional banks, but also that they will exploit the past innovations of the traditional banks.

"Absolutely. These banks will allow for more agility, in the beginning, because they don't have the physical footprint to support that we have. And they can follow some of the innovations that we've done." (Participant 3)

Participant 3, however, noted that traditional banking has been entrenched into the customer base and put forward the idea that they shall continue to operate in parallel for some time still.

"So, I think the bank probably has got a very good mix of traditional banking, as well as the digitisation perspective. There's a lot of folks out there who still want the legacy type of stuff as opposed to just digitisation. I think there's some way to go before you fully entrench the millennial into that." (Participant 3)

Two important aspects were noted by Participant 2. Those are that the elements of trust and how customers perceive, how you as an organisation is going to handle their data, eluding to the fact that trust takes time to build and the use and application of data are becoming increasingly regulated and important for customers.

"On the other side, there are risks regarding privacy and the usage of that data and using it even in an ethical sort of ways". (Participant 2)

The participant continued on the theme of trust and said the following, which implied that banks should tread carefully as trust can easily be destroyed and hamper your competitive advantage if data is not handled in a responsible manner.

"… I position myself to create trust with a customer, but yet I also want to create value-added services. And you need to balance that carefully, not to intrude on customer's and their privacy and their rights as an example, and not to create this perception that you are getting access to all of these sensitive bits of information, which obviously could be open to abuse now you don't create trust and then when that comes, often to the media, then that obviously creates a bad perception and impacts your competitive ability." (Participant 2)

4.3.2.4 *A4. Digital transformation and strategic direction*

The interviews wanted to establish if the participants believed whether or not digital transformation was essential towards steering the bank in a sustainable strategic direction. All of the participants provided a positive response to this regard. Some of the factors noted as essential towards the strategy were cost drivers and customer convenience. Furthermore, society and the bank's target market have different expectations from their banks than what they did in the past.

"Absolutely. Social society is changing so much and so is our target audiences with millennials coming into the fore and coming into the marketplace. Now, the expectations from our customers is changing completely." (Participant 4)

Furthermore, the essential requirement of being platform-based in the bank's thinking has been noted as a key criterion for success.

"Yes, I think if we want to be a bank that is that is a sustainable bank, we are going to have to become a platform bank in order to compete effectively." (Participant 5)

4.3.2.5 *A5. Senior management and strategy communication*

One of the elements that wanted to be understood was the degree to which senior management has communicated the digital transformation strategy throughout the organisation. The participants generally expressed the same sentiment that

more could be done around communication. Some noted that the frequency at which the strategy gets communicated requires improvement while others noted the level at which the communication gets pitched needs to be revisited or improved upon.

> *“I think there's a there is a huge gap between what is spoken at Group and Exco level versus what happens at a business unit level.” (Participant 1)*

> *“I think, you know, you need to have continuous engagement with senior management to say is what we want the platform to do. These are the capabilities we want to create and have that continuous engagement and then bring in, especially the risk professionals.” (Participant 2)*

Also, there seems to be a view that there is a disconnect based on what gets communicated versus how the functional implementation of it gets understood.

> *“I think there was communication, I'm not sure, people on grassroots understood it all the time.” (Participant 4)*

4.3.3 *Section B - Inherent Risk Associated with Digitalisation*

In the second part of the interviews, it was necessary to understand the inherent risk in the bank associated with digitalisation in banking. This means, that in the absence of any controls existing to manage the risk downwards, what does the risk profile of the bank look like. Put differently, if the controls are in place, are the impact, likelihood and velocity managed downwards to acceptable levels, where residual risk falls within the bank’s risk appetite.

The flow of this section of the questionnaire is diagrammatically depicted below, and the results are presented as part of this chapter.

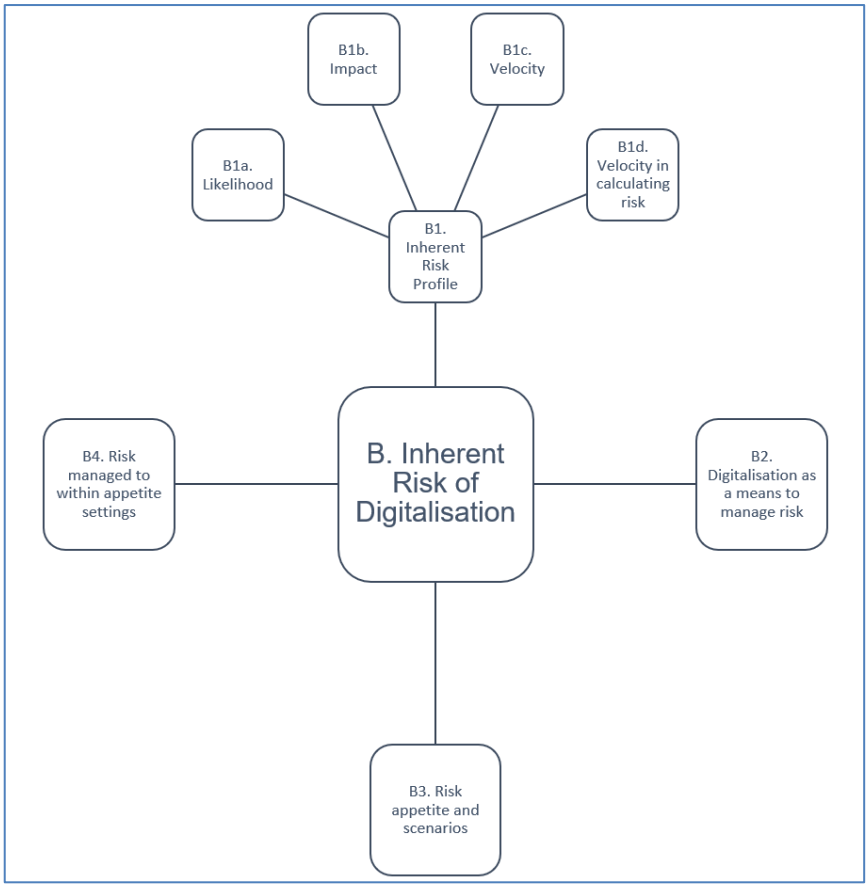


Figure 43: Inherent risk associated with digitalisation

4.3.3.1 *B1. Inherent Risk Profile*

It is important to understand how the participants perceived the overall inherent risk profile of the bank to be influenced by digitalisation. The participants all agreed that there is a definite increase in inherent risk in banking, as a result of digitalisation. Participant 1 contextualised this by adding that digitalisation brings with it new technologies and as a result, carries a high degree of uncertainty.

> *"…the mere fact the technologies have not been fully understood and a lot of it is in development. If you look at, for example, technologies that are coming out in terms of refining or producing out new solutions we're talking, for example, IoT, the actual risk has not been fully measured…" (Participant 1)*

Participant 2 cited the increasing need for data processing that increases risk, but at the same time, that digitalisation carries a need to process more amounts of personal data.

> *"Yeah, so definitely it will increase because as I previously indicated, the large-scale processing of personal data and the demands for that are different…"* and continued to add *"…digital transformation is going to get more and more hungry for personal for this data. And with that large-scale processing comes increased inherent risk for business." (Participant 2)*

Participant 4 validated their opinion of increased inherent risk because both the technology and people elements will be changing and therefore the risk inside the bank changes by default.

> *"I think the inherent risk is going to increase. So, for two reasons in that it goes to basically people and technology, our processes will get more digitized." (Participant 4)*

4.3.3.2 *B1a. Likelihood (Probability)*

As one of the three dimensions used to calculate inherent risk, it is important to understand if the participants' views on the likelihood or the probability of a risk event occurring, due to digitalisation.

All participants agreed that the probability of a risk occurring will increase, with some also commenting that both probability and impact will definitely increase.

> *"I definitely think both. I think the probability that you'd be hacked or attempted to be hacked grows, a lot. It depends on how strong your defence mechanism is. So, from a probability perspective yes." (Participant 3)*

4.3.3.3 *B1b. Impact*

The next dimension that was delved into to ascertain if there was that of impact as a determinant of inherent risk. Very similar responses were observed to that of the previous question. Participant 3, in particular, highlighted the extreme

volumes of data and the fact that it will be stored in the cloud as factors contribution to the risk.

> *"Definitely is going to be increased, the impacts of it will be higher, because now that you're storing stuff centrally storing stuff in the cloud, a lot more information tends to be uploaded into the cloud." (Participant 3)*

4.3.3.4 ***B1c. Velocity***

The third and final dimension that was being explored in the interviews, was that of velocity, where velocity equates the speed of onset of risk or put more simply, the speed at which risk approaches the organisation as a result of digitalisation.

All of the participants reacted positively to the question, by indicating that velocity would impact the inherent risk of the bank.

> *"The risk with the new technologies can actually speed up quite fast because one doesn't fully understand the cybersecurity threats behind the underlying technologies and the exposure. So just based on the velocity, the risk can materialise very quickly." (Participant 1)*

Participants 2 and 3 noted the speed element being introduced by big data, rapidly changing technologies and increasing processing power, which all directly relates to velocity and risk.

> *"I think so, I think, given the processing power of big data. Big Data has only become a technology now because of processing power. Obviously, would that you have to consider velocity, because you can just defend yourself off one attack now. And you update your software." (Participant 3)*

> *"…again, coming back to doing all this processing and using personal data as an example, speed, I mean it's, definitely fast." (Participant 2)*

Participant 4 elaborated at the speed at which cybersecurity risk now approach the bank, effectively taking the banks' exposure into zero-day scenario's.

“Now we're in the zero-day cycle, and somebody can take a product to market within a day and it can be breached within 12 hours after that.” (Participant 4)

Participant 5 noted the speed at which digitalisation now allows the industry to conclude transactions increases the risk.

“I think that is one of the key risks that we need to be aware of for digitization is that the speed in which we can conclude transactions will have a direct impact on velocity and thereby increase our risk.” (Participant 5)

4.3.3.5 ***B1d. Velocity in calculating risk***

The next question to the participants was aimed at understanding whether or not velocity was included in risk calculations, and if not, whether it should be. The participants confirmed that the bank only used impact and likelihood as determinants of risk and velocity was not currently used in its calculations.

Participant 1 confirmed that it is not currently being used and felt that it should be included as it would make for better budget and costing of risk as well as appetite setting.

“… if they understand from a velocity perspective how soon the risk could materialize, then they would be able to forecast and be able to change those amounts, as opposed to having a fixed amount constantly and that obviously has an impact on the balance sheet.” (Participant 1)

Similarly, Participant 5 also felt that the way risk gets calculated in the bank needs to be revisited, seeing that the bank is in the midst of its digital transformation journey.

“I think we will have to revisit the way we do first calculations with platform banking and apply ourselves to the newest risk scenarios that will be created by platform banking, and it may require a different way of looking at it or different risk methodology through to the traditional risk methodology that we've been adopting so far.” (Participant 5)

4.3.3.6 *B2. Digitalisation as a means to manage risk*

The participants were then asked on their views around the digitalisation of risk management tools and capabilities and whether they saw that as a means to respond better to risks, that now seemingly approach the organisation at a faster rate and also rapidly introducing new, previously unseen risks into the bank. Most participants overwhelmingly thought that this was indeed the case.

> *"Absolutely. When… when the solutions are manual, it becomes… you know, one just having to fill a spreadsheet, but when you actually use the digital solution options and technologies out there to be able to manage the risk a lot of automation comes into play." (Participant 1)*

Many participants quote the benefits of regulatory technologies and AI to combat risks as a beneficial risk management tool already in use to counteract and manage these new risks.

> *"Yes I do, I do see, we seeing examples of that right now. So for example in the anti-money laundering space. We have through artificial intelligence created efficiencies, we can identify risks much quicker we're not so, we're not so limited by manual interventions etcetera. And that positions us to be able to respond quicker to some of the threats we face as a financial institution." (Participant 5)*

4.3.3.7 *B3. Risk appetite and scenarios*

The question posed to the participants was whether they thought that the bank's risk appetite and future risk scenarios have planned by taking the risks associated with digital transformation into account. To this question, most of the participants felt that some work is being done around this, but that it can be enhanced or improved upon.

> *"So, I would say group level. Yes, but there could be more work, meaning more input into that risk appetite development methodology." (Participant 2)*

“There's a lot of work to be done. And that's because although technology is moving very fast. People don't change as quickly as they otherwise could show the take on is erratic through the bank, but it's happening.” (Participant 4)

“Yes, I do, I do see, we seeing examples of that right now.” (Participant 5)

Participant 1 felt that it is currently not being looked at, at all.

“No, I don't believe that they have done that because I have not seen from where the bank actually does measurement when currently the measurement of risks and how it's measured and the way it gets captured…”. (Participant 1)

4.3.3.8 *B4. Risk managed to within appetite settings*

In this final question of this section of the questionnaire, the participants were asked to consider the residual risk associated with digitalisation and whether they were of the opinion that the risk was sufficiently managed downwards in terms of the bank’s risk appetite.

The generally shared view amongst the participants was that a current work in progress and that some improvement is required in this space. Participant 5 noted the following.

“So, we building the plane, while we're flying it.” (Participant 5)

4.3.4 *Section C - Risk Response and Risk Management (Digital Skills & Tools)*

In this section of the interviews, it was necessary to understand the risk response and risk management strategies that the bank has in place as it relates to digital tools and skills. Digital tools and skills form an important part of how an organisation is geared to respond towards and manage risks.

The flow of this section of the questionnaire is diagrammatically depicted below, and the results are presented as part of this chapter.

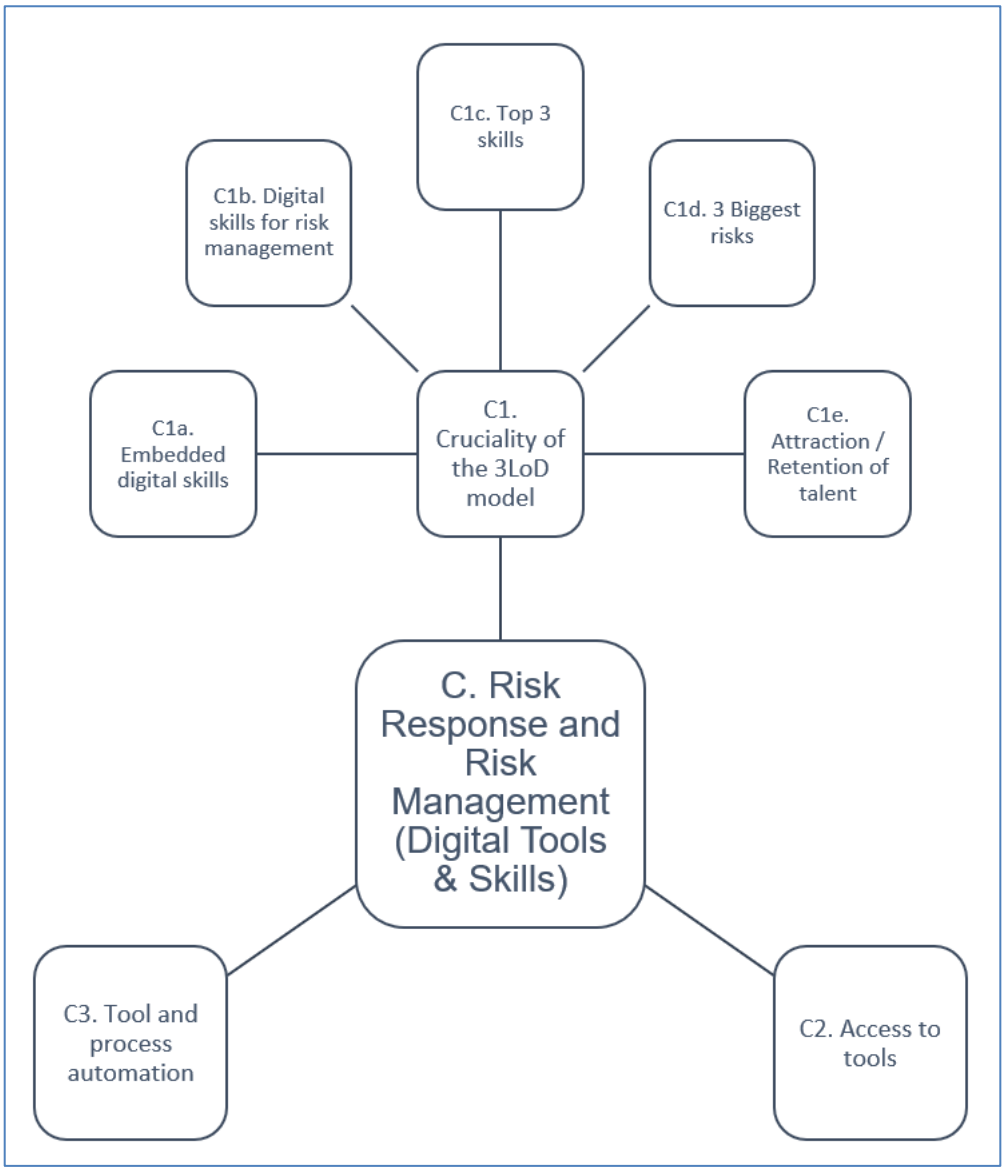


Figure 44: Risk response and risk management (Digital skills & tools)

4.3.4.1 *C1. Cruciality of the 3LoD model*

The first part of this section of the interview revolved around the 3LoD model. It was necessary to establish if the participants felt that the 3LoD model was crucial towards managing risk, both traditionally and going forward as the bank goes through the digital transformation process.

The participants felt that the 3LoD model was crucial for proper management of risks, but some noted that improvement was required in some areas especially where digital skills are concerned.

Participant 4 in particular again noted the volume and variety of data that we deal with, noting that the 3LoD model is critical if we are going to manage risks around this.

> *“Yes, it's not even a question. Okay, and especially with such a volume of data. And the within the volume. It's easy to hide small things. And because there is so much and it's easy to hide a small thing, a small thing can have a very large venue and in a very large impact. So, if we lose sight of those three lines of defence we're not going to review ourselves.” (Participant 4)*

And Participant 5 had the view that right now, the model is sufficient.

> *“Right now, it seems that the three lines of defence is kind of the way we deal with risk in an organization. And it works, and I think they will still be a long time for which it will work it will continue to work.” (Participant 5)*

4.3.4.2 ***C1a. Embedded digital skills***

The next question wanted to understand if digital skills where embedded across the 3LoD in the organisation.

The participants all felt that there were some elements of embedded skills, but that improvement was required.

> *“Currently, as it stands, the bank is, they have the necessary skills to cope for the current environment. But going for the future and developing the individuals for the future, a lot more effort needs to be put in from the bank to support the individuals who need the necessary skills to be prepared for the future. So it works much with the bank versus the employee having to meet on middle ground and understand the impact that the risks will actually the digital technologies or the type of risk that these technologies*

will introduce into the environment is going to be totally unique and different. And the skills currently, I believe that staff are not adequately ready to take on what's to come." (Participant 1)

And with Participant 2 adding the following.

"From a shared line, no. I know I shouldn't say blanket, no, but not everyone." (Participant 2)

4.3.4.3 *C1b. Digital skills for risk management*

The next question wanted to know if participants felt that having digital skills across the 3LoD in the organisation was crucial, in order to manage the risk associated with digitalisation. There was consensus from the participants that digital skills were indeed crucial, noting that job functions and expectation are changing as technology is changing the way we work and respond to risks.

Participant 4 felt that it is crucial that staff are multiskilled and that it is no longer just sufficient to say that you are knowledgeable in your specific field. The Participant added that in order to manage risk holistically, shared knowledge of various functions is required if you are going to manage risk successfully during digital transformation.

"So, an understanding of the subject matter that the digitization is enabling, the digital enabler are going to be paramount. So, having somebody in IT, who doesn't understand business, and the business outcomes is no longer going to be okay. We're going to need people to understand, both business and the technology." (Participant 4)

4.3.4.4 *C1c. Top 3 skills*

The next question, as can be expected had some mixed responses where the participants generally seemed to favour skills that were more closely aligned to their job roles and functions.

“Well, the first is coding and development. The second is a technical understanding of neural networks. And, the third is actually having the ability to conceptualize.” (Participant 1)

Participant 2 felt that understand of data and data science was crucial, not at an expert level but that staff needed to have the ability to work with and interpret data.

“I would say some sort of, I can say introductory, data science-related skills. I'm not saying be everyone has to be a data scientist…” (Participant 2)

This was also echoed by Participant 3 and Participant 5.

“I would definitely say data analytics. Definitely engineering from a process perspective. And given our discussions now I would definitely say risk, but risk from a perspective of a digitally savvy risk function.” (Participant 3)

“I think data is big, so it would have to be data analytics. I think we would need. We would need risk managers who are able to bring a data component into the work, not you know traditional risk managers, probably didn't need to consider that. But if everything is going to be data-driven.” (Participant 5)

4.3.4.5 ***C1d. 3 Biggest risks***

The next question that was discussed was what the participant thought were the top 3 biggest risks that faced the organisation during its digital transformation journey.

Participant 1 noted the concern around not having basic technical skills or understanding of the technology and further noted that people having access to that technology is crucial, which will create a risk in itself if it was absent.

“A key risk is basically not understanding the technology properly, right. The second risk will be the technical skill that's not available. And the third,

I would say is that the technology may not be easily or readily accessible." (Participant 1)

Participant 2 felt strongly that the biggest risks we face were that around data and data privacy, especially when it comes to dealing with data privacy breaches and cybersecurity threats.

> *"The top risk would be relating to like I think I alluded to earlier, concerns relating to data privacy and protection under the protection of cybersecurity threats." (Participant 2)*

Participant 3 noted a miscommunication or disconnect in the digital transformation strategy. Noting that the organisation will operate in this parallel world where there is a very traditional operating model that you are trying to digitally transform yet your defence model is not aligned to deal with the new digitalisation risks.

> *"I think the ones that come to mind is definitely, you're not having your defence mechanisms in sync with what your business strategy is, touch on the previous discussion earlier. You can try and position yourself as a digital-savvy organization, but your defence mechanisms are very traditional in nature…" (Participant 3)*

Participant 4 was of the view that the biggest risk was not digitally transforming as one organisation as a whole, eluding the fact that the digital transformation strategy across the organisation is crucial and that fragmented implementation of digitalisation will introduce risk.

> *"We one part of the bank is taking on the digital transformation a lot faster than another. So, you'll have one part of the bank speed up and keep up to date with it. And another being left behind. And with that separation, you're going to get a disconnect within the environment itself. The costs for digital security are going to increase exponentially." (Participant 4)*

Participant 5 noted that the diversification of services away from traditional banking coupled with the high regulatory risk environment withing which banks traditionally operate will create complexity and introduce risks.

> *"General risks that we face, which will still be there whether it is a fourth industrial revolution or not is the regulatory risk, the compliance with, you know, the massive mass huge amount of legislation that we have to comply with. And with us being a group that has different services are not traditionally banking services. We just don't deal with banking-related legislation we deal with other legislation as well. Model risk for me is a key thing and I think it's cyber risk." (Participant 5)*

4.3.4.6 *C1e. Attraction / Retention of talent*

The next question dealt with the attraction and retention of talent. It dealt with the need for organisation in an increasingly competitive and fast-paced environment dealing with the competition amongst banks for skills. Participants were requested to give their views on whether or not sufficient work was done in this area which ensures the attraction and retention of top skills to ensure the digital transformation risks are managed.

All the participants noted that there is improvement required in this area, which is probably a function of competition, implying that all organisations would be struggling with this issue.

Interestingly, Participant 4 also cited the economic and political environment in South Africa which is resulting in a brain-drain of skilled resources.

> *"I think we're doing what we can. But the political climate in South Africa is meaning that key staff are not being lost to other banks. They're being lost to other countries, and worldwide there is such a shortage of skills and knowledge." (Participant 4)*

4.3.4.7 *C2. Access to tools*

The next question in the interview asked the participants if they were of the view that staff have adequate access to tools to sufficiently digital transformation manage risks.

Though most participants felt that more work is required in this area, Respondent 5 noted that as a large organisation there is a centre of excellence that has been set up to assist individual areas where necessary.

> *"I think we have access to the centres of excellence that can assist us. I think that we need to capacity our teams with those type of skills." (Participant 5)*

Participant 1 had the view that a deeper understanding of the use cases and the risk was required before it could be said that the functions were adequately equipped with the right tools.

> *"I think they have the necessary tools to manage existing risk, but what digital transformation… the toolset has not properly been defined. So, in order for you to actually make use of necessary tools, you need to know what tools are needed to manage the transformation to a particular technology, but to understand the tools that you require, you need to understand the use cases that's required or the use cases that will evolve out of these new technologies." (Participant 1)*

4.3.4.8 *C3. Tool and process automation*

The final question in this section dealt with the fact of whether or not risk tools and processes were sufficiently digitised or automated within the organisation. All participants agreed here that improvement was required across the organisation to fully automate risk tools and processes.

> *"Definitely not. I think there's a lot more work and effort that can be introduced. But if you actually try and digitize the existing tools, I believe that you will only reach a particular cap. And meaning that those tools will*

have a limitation of what it can actually do when you're trying to digitize a particular tool." (Participant 1)

Participant 3 further elaborated on this noting that traditional audit functions still heavily rely on spreadsheets instead of using automated tools and process.

"I think risk internal audit is very synonymous with Excel sheets. And I think that's part of the deciding factor." (Participant 3)

4.3.5 *Section D - Risk Response and Risk Management (as it relates to types of risk)*

In the final section of the interviews, questions were posed to the participants to understand the bank's risk response and risk management strategies as it relates to different risk types.

The flow of this section of the questionnaire is diagrammatically depicted below, and the results are presented as part of this chapter.

Figure 45: Risk Response and Risk Management (as it relates to types of risk)

4.3.5.1 *D1. Cybersecurity*

The next question that was posed to the participants was to provide insight into their views on the bank's ability to monitor, detect and respond to Cybersecurity threats.

Overall, the participants tended to agree that the bank was resilient and have the right systems and algorithms in place to manage and prevent attacks. But there was a sense of caution as all the respondents felt that this was unchartered territory and that no one is really safe from a cybersecurity attack due to the ever-evolving hackers in this space.

Participant 1 felt that even though the bank was probably the best in the market in terms of being the least vulnerable to attack, that some improvement is still required as was proven through penetration testing exercises that were done in the bank.

> *“We know that other banks are more susceptible, we've had pen tests done on the bank, and the bank has proven to actually have weak points, which can be easily exploited should threats become more vicious, more text towards the bank.” (Participant 1)*

Participant 2 felt that we were well and adequately resourced, but the nature of this threat meant that continuous improvement is always required.

> *“I think we've got good capabilities. I think we can definitely identify them we can respond to them. From where I sit, I think we are properly resourced. Yes, they are. are always enhancements that we can do, especially in terms of Information Security Management Systems.” (Participant 2)*

Participant 5 added that the resilience is there but that the organisation must not sacrifice this in rush to market with new products or whilst it is on the digital transformation journey.

> *“I think we are quite resilient, there was a denial of service attack quite recently which we've managed to successfully control. I think we do have the right skills and the right tone from the organization. My concern is that we If I can call them the hackers out there are very smart. And that one day they will manage to penetrate the organization. I think as we go on this digitization journey one of the risks for me or one of the things that keep me awake at night is our, our rush to get to market with some of our digital products.” (Participant 5)*

4.3.5.2 *D2. Crisis management and business continuity management*

Next, the question was asked on what the participants thought about the bank's ability to perform crisis management, business continuity management and disaster recovery.

All the participants were of the view that the bank is fairly mature in its ability to respond to a crisis. Some concerns were raised in terms of responding at an organisational level, due to the size and complexity of the overall group.

Participant 4 voiced the view that the bank's greatest asset is its people and their resolve and spirit of innovation to overcome problems during crisis times.

> *"And we actually are incredibly mature. But nothing's written down. We've got amazing people who can respond intuitively. So, the way our war rooms are being run. When business continuity comes up. We tend to be very ingenious and innovative at that moment in time. And one of the things the bank's culture now is our people. At that moment in time to respond really quickly, and outside of the process and because of that, our ability to continue performing in the case of a high critical incident is incredibly high because we allow our staff to do that." (Participant 4)*

4.3.5.3 *D3. Data Governance and Privacy Laws*

The next question asked to participants was what their opinion was on the bank's ability to comply with data governance and privacy laws.

Most participants felt that the ability of the bank has not fully been tested as there has neither been a major incident nor has the legislation in terms of POPIA come into full effect yet.

> *"I think with the recent introduction of various policies and defining certain procedures, the bank does have these in place to address it from a governance perspective. However, these policies and procedures have not been properly tested because they have not been threats." (Participant 1)*

Participant 2 elaborated further on this point, noting that the delays in the implementation of the regulations have probably allowed the bank to take its foot off the accelerator.

> *"… implementing of the controls, although it is underway to comply with data privacy laws like POPIA, … it doesn't give you that momentum to speed up the implementations which might change now in April when they assume that POPIA will come into effect." (Participant 2)*

Others were of the view that the bank is sufficiently prepared to respond to what the regulations require them to do once it comes into effect.

> *"I think there is a right focus and attention to it. We have been dealing with it for a while now, and POPIA is at the stage, where it should very soon become law." (Participant 5)*

4.3.5.4 ***D4. Protection of customer data***

The confidence of the participants in the bank's ability to protect and safeguards its customer's data was tested next.

All participants were of the view that the intent and commitment were there and there will always be an element of doing more than what you are currently doing. This can most probably be attributed to the inherent nature of data and big data in the sense of digital transformation.

Participant 3 and 5 specifically credited the bank's commitment to have accountable individuals at a business unit level to take ownership of customer data. Participant 3 also highlighted, by way of example, the tremendous focus that the bank placed on achieving Payment Card Industry Data Security Standard (PCI DSS) compliance, which spoke to the minimum information security standard required to handle credit card information in the industry.

> *"Yeah, I definitely think so. I think if you look at the focus on PCI. I think that's one of the biggest ones around credit card numbers. The fact that they use tokenisation in tackling each position with information from each business unit, and in most cases, the information owner has to be the CEO*

of their business or an Exco member from that business unit is the right way of going about it." (Participant 3)

Participant 5 mentioned the commitment around the ownership at a business unit level but noted that more effort is required in this space.

"I think the commitment is there. We do have to mature around the appointment of our data stewards and our custodians in the business and making sure that they know what their obligations are in terms of the data. I think there's a piece of work to be done around that. But the intention is there, the commitment is there." (Participant 5)

Participants 1 and 4 were of the view that there is some good practices, systems and controls in place but eluded to the fact that some smaller systems create loopholes and information to leak out of the organisation in some instances. Participant 1 further noted that the data strategy overall will need to evolve with the evolution of digital transformation, as the nature of data is changing.

"We have certain measures in place, we have monitoring in place, even though the monitoring might not be a hundred per cent safe, and there is still a loophole for information to go out. These are prospective controls for now for the current situation. So that obviously needs to be expanded, interrogated and see what alternative approaches and that comes in with digital technologies that you will introduce." (Participant 1)

"In the big systems, yes. Overall, no. And that's one of my top concerns." (Participant 4)

4.3.5.5 ***D5. Cloud Infrastructure***

The next question looked into the participant's views on the bank's ability to secure its cloud infrastructure.

All participants expressed satisfaction with the bank's competence around this, especially noting the attention that cloud infrastructure is getting from a governance perspective and that there are dedicated committees in the group towards ensuring the security around this initiative.

"… so the bank has put in place various governance-related controls around cloud access standards and policy for cloud-type solutions. The Reserve Bank has also published directives that we comply with as it relates to cloud and offshoring and outsourcing of whatever services that involve data to a cloud provider. So governance controls are in place." (Participant 2)

"So, the bank has the cloud steerco, and my understanding… of that steerco's obligations or accountability is that they need to review every application for any storage in the cloud be it our own cloud or any third-party cloud. So, I'm comfortable that if that steerco exercises its duties properly. That there is proper governance around it." (Participant 5)

Participant 1 further noted that in some instances more testing an assurance needs to be provided that information and data that gets uploaded or processed in the cloud needs to be protected.

"The bank has a forum currently that looks at cloud technologies. They have the forum to actually review cloud technologies and propose different solutions and recommended solutions. So, I think they are adequately geared to introduce cloud technologies. However, in some instances, they have not properly tested and looked at every possible scenario, their quickest ways having to restrict information to protect it." (Participant 1)

4.3.5.6 ***D6. Third-party risk***

The next point in the interviews explored whether the participants believed that the bank managed its third-party risks sufficiently.

All the participants felt that this was an area where there was definite room for improvement and was insufficient in some areas.

"I don't think that it is sufficient. I think that it is…It is minimum. A lot of it goes on trust. That's what the bank needs to really experience is when they engage with a trusted party, and that party gets breached, then it has a huge impact." (Participant 1)

Participant 2 further elaborated by stressing the importance of managing this risk at a supplier and procurement level for the group, implying that stricter due diligence is required to manage third-party risk.

> *"So, so, at this point in time, not sufficiently, there is more work that is underway to enhance risk assessment, and management of suppliers. From a data privacy and protection point of view, we've been very vocal with our procurement colleagues to put the proper risk assessment in place especially for data privacy and protection." (Participant 2)*

4.3.5.7 *D7. User access*

The bank's ability to manage and secure user access and identities was the next question that was posed to the participants.

The participants were of the view that more could be done in this space. Stressing for example that it is an ever-changing environment that is highly dependent on individual maturity and accepting responsibility for password and security management of their systems access.

Participant 3 noted that using technologies to ensure the robustness of controls will assist the bank in managing this, citing specifically two-factor authentication.

> *"I think its as proper as it's going to get. I don't think you can hold a bank responsible if I share my password with someone else… this is an irresponsible employee. But apart from that, I think in most cases the two-factor authentication is coming out, helps a lot." (Participant 3)*

Participant 1 also found that the system may be sufficient for the current situation but that it is not geared for full-on digitalisation.

> *"And the systems that we're using now, as it is the bank has the ability to monitor and manage user access on the various platforms, grant access, restrict, remove access, but it is not managed from a futuristic perspective..." (Participant 1)*

Participant 5 further elaborated on the dynamic nature of this security portfolio, stressing that it is an evolving function.

> *"Now I think we can be there is an improvement on user access and identification and revocation of access is an ongoing project in this bank. We recently made really good strides in cleaning up that portfolio. To the extent that it's now marked as green, but it is an ever-changing portfolio." (Participant 5)*

4.3.5.8 *D8. Digitisation of business processes*

The next question tested the views around the bank's maturity around the management of manual process digitalisation.

Across all the interviews with the different participants, there was consensus that the bank lacks maturity in this space and that this is a definite area of improvement.

Participant 1 expressed the fact that the bank will only allow digitalisation once the technology has proven itself to outperform the manual and trusted processes that are currently in play.

> *"No, I think the manual business processes will always be there. Because the bank is a very untrusting entity, it doesn't trust easily. So it will still be highly dependent on people until the technology has been proven by a million other entities focus a million but what I mean is many other entities until that technology has been proven and stable enough and robust enough to be introduced into a bank." (Participant 1)*

Participant 2 and 5 noted that in some areas manual processes are being reduced by using automation, but that it is still a work in progress and further noted that there is a need for a centralised view of process automation.

> *"So, in terms of manual, they are not mature but they aren't getting there. So, using technologies such as RPA, robotics process automation, to try and eliminate some of the manual work." (Participant 2)*

“I think there's a lot of work to do in terms of realizing the required level of maturity that we want to have. I think we are still immature; we are still manual, and we don't have a centralized view.” (Participant 5)

Participant 3 and 4 further added to this view by noting that the business is automating as fast as it can, given the restrictions, resource capabilities and challenges that it has.

“I think there's a lot of manual processes, hidden behind them. Yeah, and I think it's a case of, we will digitize as much as possible as fast as possible to keep up with the market.” (Participant 3)

“Incredibly weak. So, because our resources are so limited, and we focused on the big-ticket items. Saying that we're weak, doesn't mean we're bad, it might be a risk that we've chosen to accept because the big-ticket items are just so big.” (Participant 4)

4.3.5.9 ***D9. Compliance and regulatory programmes***

The next opinions that the interviews aimed to understand was whether the participants thought that the bank ran a modern compliance programme.

Amongst the participants, there was a mixed response to the question. Two participants felt that the compliance programme in the bank was modernised and was geared well to respond to the challenges faced by the bank.

"Yes. So, we have set up I think quite a… if you want to call it a modern foundation and basis for compliance programs. Setting out how they should be structured and your various elements to compliance with the programme..." (Participant 2)

"Yes, I do. I think we have a very mature compliance program, it is not an easy portfolio, because the environment… the regulatory environment is constantly changing and the threats against us evolve all the time." (Participant 5)

Two participants believed that it was done well but that there is room for improvement in terms of modernisation, with Participant 4 again stressing the importance of looking at velocity in terms of the speed of onset of new risks.

> *"So, at the face of it you could say yes, but how we actually execute on it, and the back end is still lots of pushing paper..." (Participant 3)*

> *"We can see regulatory changes overseas happening a lot faster. Like the growth of GDPR versus the growth within POPIA. So, GDPR has moved a lot faster than POPI has. And those compliance requirements, as we hit the digital age, we are becoming more global. So, we're going to have to speed up, but I don't think it's there yet, but this, in my opinion, is where velocity comes in again." (Participant 4)*

Participant 1 had the view that the compliance programme in the bank was not modernised at all, noting that the compliance programme was a function of the slow-moving regulatory environment within which the bank operates and dominated by a lack of digitalisation on the governments part.

> *“I won’t say a modern compliance program, I think it's a compliance program, because if you look at our regulatory… government has not yet put that into… into a digital frontier.” (Participant 1)*

4.3.5.10 ***D10. Senior management support of risk***

This question wanted to understand the degree to which senior management and executives support the risk management function in the bank.

Overall, the participants felt that more could be done in this space. It was noted that there was support at a very senior level but in between different segment and business units in the bank, it was quite fragmented. This meant that you would have great support from management in one area and have a very different level of support in another.

Participant 1 noted that strategic alignment was crucial for the buy-in from senior management, noting that in the absence of that senior managers would not support the risk function.

"I think to a certain extent, they will support if it aligns to their way of thinking and the particular strategy." (Participant 1)

Participant 2 noted that there is support, but getting the right resources allocated to the function to ensure that it is mitigating the risk sufficiently is a problem.

"I think they support that they do support the second line. They do know that the compliance risk is a reality and needs to be mitigated. That's what I pick up sitting at a group level. However, coming back to the allocation of resources…to put that control environment in place, that compliance-controlled environment, is a challenge." (Participant 2)

Participant 3 noted that the way in which the risk management function operates may be a cause of frustration for business executives. Closer alignment in terms of ways of working, such as digitising the risk management function, could solve this problem.

"I think they definitely aware of it, and I think they definitely understand the risk involved. But I think the manner in which risk operates within the processes. I think from, that's probably a limiting factor in business working hand in hand with my personal view is. I think, as soon as risk comes in with spreadsheets, and in business tends to see okay… should I now be required to log these identified risks. So, I think that's where the digital-savvy will definitely enhance that relationship " (Participant 3)

Participant 4 highlighted the different levels of support observed throughout the organisation, highlighting the fragmented and siloed approach that exists throughout the organisation.

"The risk management function, I experienced in previous iterations, did not get the full support. But in, in my experience, it was because risk was not seen as part of the business. It was seen more as a policeman, somebody who got people into trouble. Within this segment, I'm seeing a very different profile starting to emerge where the risk people are seeing themselves as a line of defence, not an attack." (Participant 4)

4.3.5.11 *D11. Mobile workforce*

The final question touched on whether the participants believed that the bank has fully embraced a mobile workforce.

Overall, the participants felt that the bank had a clear mobility strategy in place, but that in some areas, depending on the personal view of the manager, the bank could improve on its mobility policy.

> *"I think, again, this is a journey. It starts somewhere. The bank has just started introducing working remotely. But a mobile workforce can mean many things in different areas. For one team, it could be going out there and remotely supporting a team's you don't need to be physically present." (Participant 1)*

Participant 2 noted that this is crucial for productivity and stressed the benefits that this will have on the organisation.

> *"They starting to, they started, and I mean, I'm positively impacted by it. So yeah, and I think we need to get there because having mobility is, I think is in this day and age is key to productivity." (Participant 2)*

Participant 3 noted that across generations and depending on an individual's tenure in the bank, they might not embrace mobility due to their own beliefs and convictions.

> *"Yes. Definitely the younger generation. I don't really want to say millennials… still, a lot of people with tenure long enough in the bank to have this perception that if I don't see my employee present then they may not be working. We've definitely done a lot better than most organizations. We manage on outputs, rather than personally present." (Participant 3)*

Participant 5 noted similar views to that of participant 4, adding that the support from top management is indeed there and part of the bank's strategy, but at a business unit level some managers were still struggling with the concept.

"I don't think we have embraced it yet. I think we are getting there. I think our CEO has been driving it quite hard. And there are still some managers that are a little bit traditional thinking, I had to also wrap my mind around this concept of having a team but not to ever seen me." (Participant 5)

Participant 4 noted that the bank's human resource practices will be crucial to manage the mobile workforce in terms of onboarding new staff and performance management.

"I think we have. I think there's a lot of maturity, as I said before, the maturity is going to come in our HR practices, and who we hire and how we hire. So, moving from a time, a traditional time-based methodology in terms of people to quality is going to be difficult. But I think we're embracing it, these are challenges we're going to have to accept." (Participant 4)

4.4 Summary of the results and findings

The chapter highlighted the results from the qualitative data that was collected. The basic results from the statistical analysis were first presented, indicating the different responses that were collected using the questionnaire that was constructed in four parts, i.e. The fit for future assessment, the perceived inherent risk in the organisation as a result of digitalisation, the digital risk assessment and the measurement of the organisations risk response and risk management readiness.

The results from the questionnaires was also used for the detailed statistical analysis that looked at the data using correlational analysis, general linear modelling ANOVAs to assess relationships between demographics and main variables, structural equation path modelling with latent variables (SEM), and moderated mediation (Hair et al., 2009).

The data collected from the qualitative interviews was then presented, highlighting the participant responses, that were coded using thematic data analysis. The data was obtained through semi-structured interviews that followed

a similar format to that of the quantitative questionnaire but allowed for open-ended discussions.

The interviews were structured to allow for the feedback to be categorised in four parts, i.e. understanding the digital transformation journey of the organisation, understanding the perceived inherent risk associated with digitalisation in the organisation, and the final two-part which looked at the digital response and risk management in the organisation. The last two parts of the interviews had a focus on skills and tools used to manage risk in the organisation, followed by a section that looked at the organisational response to digital risk factors.

The results from the qualitative and quantitative analysis will be discussed in Chapter 5 hereafter, in conjunction with the reviewed literature.

5 DISCUSSION OF THE RESULTS OR FINDINGS

5.1 Introduction

The research paper started with an overview of digitalisation and the challenges that that banks in South Africa, may face in terms of digital transformation and risk management. This was framed within the context of the fourth industrial revolution and the various digital transformation journeys that organisations, and in particular banks are embarking on in South Africa.

The concept of velocity as the third dimension of risk management was introduced in order to explore the merits of evaluating risk using three dimensions instead of the traditional two dimensions. The ability of banks to appropriately respond to digital risks as it relates to skills and tools was then explored.

Chapter 4 presented the results from the findings of the research, as it pertains to the two research propositions, i.e.:

i. Proposition 1: There is an increased inherent risk associated with digitalisation in banking, as digitalisation increases the impact, the probability and the velocity at which risks approach the banking industry.
ii. Proposition 2: Banks in South Africa are prepared to respond appropriately to risks that result from digitalisation, as they are sufficiently skilled and have the right tools to perform their duties.

In this current chapter, the results from the analysis in relation to the theory is being discussed.

5.2 Discussion pertaining to Proposition 1

5.2.1 *Overview: Proposition 1*

Proposition 1: There is an increased inherent risk associated with digitalisation in banking, as digitalisation increases the impact, the probability and the velocity at which risks approach the banking industry.

The results as it pertains to Proposition 1 is discussed as per the highlighted sections of the figure below.

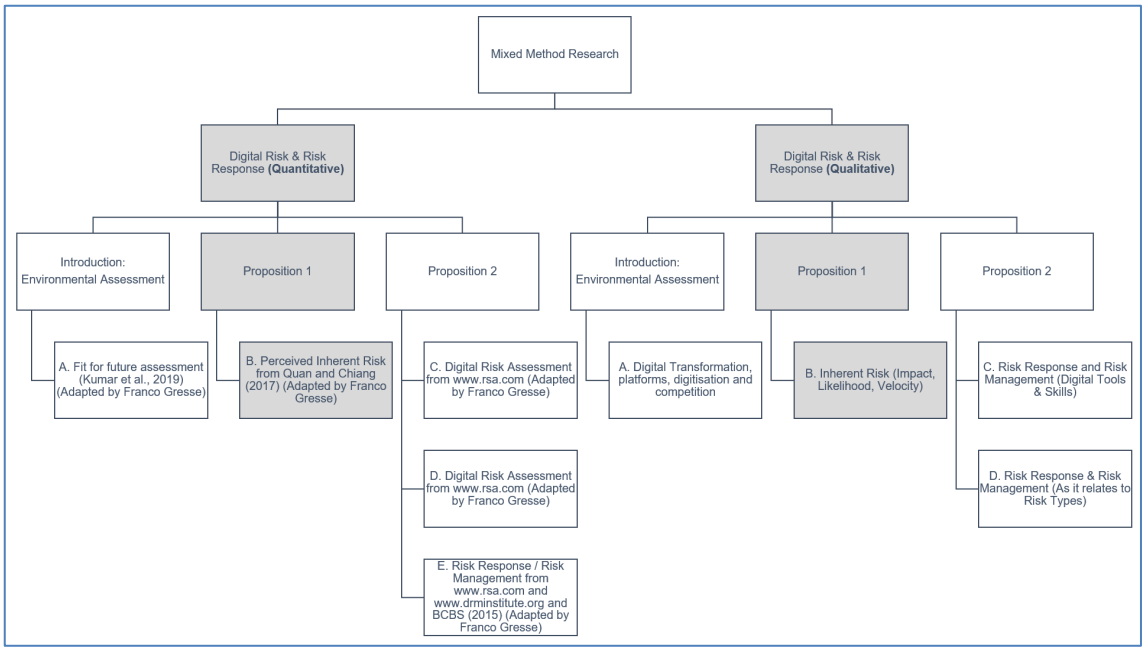


Figure 46: Discussion of Proposition 1 in relation to theory and research findings

5.2.2 *Discussion: Proposition 1*

5.2.2.1 *Likelihood or probability*

All the participants in the interviews also agreed that the likelihood or probability of a risk materialising will increase. The quantitative data revealed that the respondents agreed and strongly agreed, with a collective 53% indicating that they believe that the impact would increase as a result of digitalisation.

5.2.2.2 *Impact or consequence*

There was full agreement amongst all the participants in the qualitative interviews, that that the impact or consequence of a risk, will increase due to digitalisation. Similarly, the quantitative responses collected revealed that 82% of respondents felt strongly or very strongly that impact would increase. This was supported by the correlation analysis, which showed that risk is significantly related to perceptions of impact ($r = .70$, $p < .01$) and the structural equation model that showed Risk is related to impact ($\beta = .65$, $p < .01$).

5.2.2.3 *Velocity or speed of onset*

The results from the qualitative interviews revealed that all the participants agreed that there is an increased risk associated with velocity or the speed at which risks will approach the bank as a result of digitalisation. Again, similarly, the quantitative data revealed that 76% of respondents were of the opinion that velocity would increase as a result of digitalisation.

All the participants also agreed that velocity should form part of the risk calculations going forward.

5.2.2.4 *Inherent risk*

The qualitative data revealed that all of the participants agreed that there is an increased risk associated with digitalisation in banking. Based on the responses collected in the questionnaires, the respondents revealed an overall increase in perceived inherent risk as well.

As part of the risk assessment, the inherent risk was calculated using the proposed model of Quan and Chiang (2017), who expressed this in a mathematical formula, i.e. Risk = (Impact x Likelihood) + Velocity. This revealed that as a result of digitalisation, the organisation's perceived increased inherent risk was positioned at the very high and extreme ends of the scale, with a collective 51%. A further 19% was rated as high and the remain 30% as low and medium collectively.

According to RSA Security (2019c), the velocity and impact of risk associated with connectivity will drastically increase. From the correlation analysis, it was revealed that digitalisation is significantly related to perceptions of risk ($r = .26$, $p < .01$). The noting of the participants in the qualitative feedback of especially concerns around data and cybersecurity underscores this risk around impact and velocity. Both big data and cybersecurity carry inherent characteristics of velocity. Big data has a dimension associated with velocity, which refers to the speed at which data gets processed (Chen et al., 2012; Gandomi & Haider, 2015). Similarly, cyberspace carries the characteristic of the speed of processing (Clemente, 2015). It then seems almost obvious that the dimension of velocity should be used to calculate risk, even though from the qualitative interventions, it was determined that this is not currently happening.

For a bank that is in the midst of digital transformation, this should be concerning. According to Rogers (2016) and Ismail et al. (2014), companies that will be successful in their digital transformation efforts are the ones that incrementally take risks, which in turn enables a culture of innovation.

Failure to correctly calculate risk may result in overexposure and eventually in financial and reputational losses. Similarly, overstating risk and therefore foregoing new business opportunities may result in failure to digitally transform, provide competitive offerings to customers, and remain relevant in an ever-increasingly digital space.

5.2.3 *Conclusion: Proposition 1*

According to Weichert (2017), there are many factors that are driving the digital transformation in the organisation and amongst these driving forces are customer needs, new disruptive technologies and cybersecurity and risk management.

The proposition that there is an increased inherent risk associated with digitalisation in banking, is therefore positively supported by the qualitative and quantitative research undertaken in this study.

The results and analysis have proven that digitalisation increases the impact, the probability, and the velocity at which risks approach the banking industry.

5.3 Discussion pertaining to Proposition 2

5.3.1 *Overview: Proposition 2*

Banks in South Africa are prepared to respond appropriately to risks that result from digitalisation, as they are sufficiently skilled and have the right tools to perform their duties.

The results as it pertains to Proposition 2 is discussed as per the highlighted sections of the figure below.

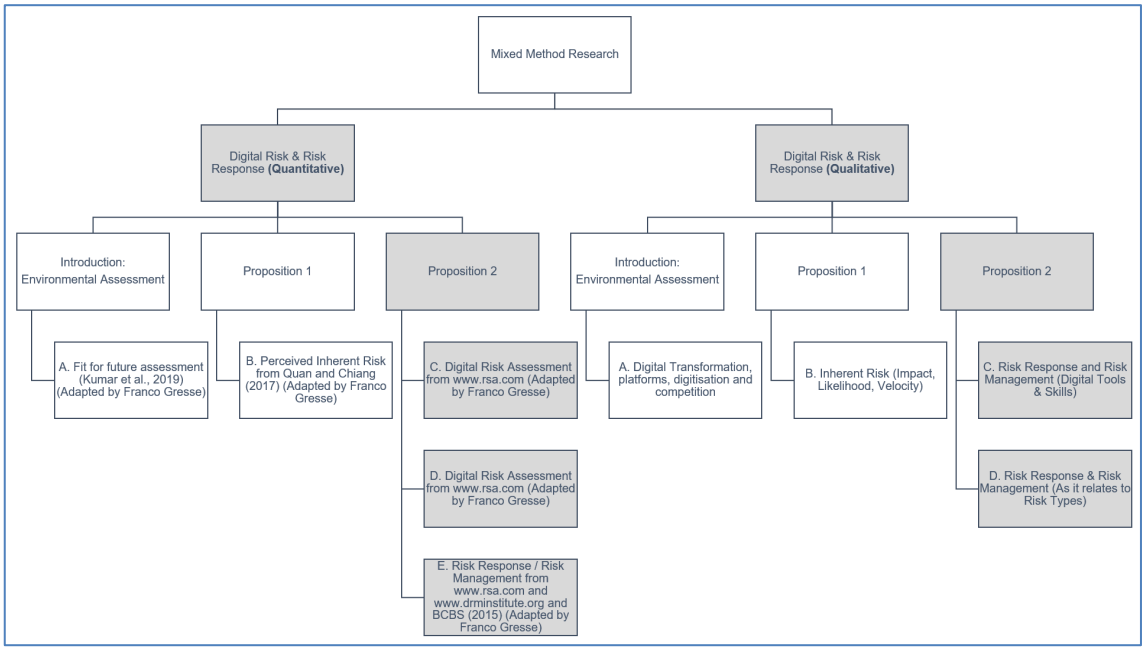


Figure 47: Discussion of Proposition 2 in relation to theory and research findings

5.3.2 *Discussion: Proposition 2*

5.3.2.1 *Digital skills of the 3LoD in banking*

The qualitative study revealed that the 3LoD is still the go-to and preferred model for managing risk, even during digital transformation. The integrity of the banks' 3LoD model was backed up by the survey respondents of whom 58% strongly agreed that the bank operates under an independent three lines of defence model. A further 27% indicated that they somewhat agree, with the remaining 15% being either neutral or not agreeing. This means that there are agreement and acknowledgement as per the guidelines from the Basel Committee on Banking Supervision (BCBS) (2015), that banks in South Africa need to run independently, three lines of defence in order to manage risk successfully. From the qualitative interviews, the data collected however found that digital skills are not fully embedded across the three lines of defence and the bank should focus on developing that across all three lines.

There was agreement that digital skills are crucial for future risk management in the bank. Data and analytical skills were especially highlighted as being crucial in digital transformation. IRMSA (2020) noted the important role that risk management plays in digital transformation and highlighted the critical need for data analytics and quantitative capabilities, which supports the proposition in this sense. This substantiated through the need for faster decision making as the speed at which risks approach the bank in digital transformation has been acknowledged (IRMSA, 2020).

The top risks that face the banking industry today have been noted to be that relating to data, data privacy and cybersecurity (Clemente, 2015). Again, stressing the point that in order to manage these risks effectively, skills across the three lines of defence in the bank would need to be developed to address them.

A concerning point is that the participants in the qualitative study all noted that more could be done in order to attract and retain talent. This risk, was one of the stated risks highlighted by IRMSA (2020), having stated that the failure to develop, attract and retain talent would be a nationwide problem. Furthermore,

the fit for future assessment adapted from Kumar et al. (2019), revealed that only 7% of respondents were of the view that the bank regularly trains, upskills and invests in learning and development of digital technology. Another group of people making up 38% believed that the bank was in the middle of the pack when compared to its peers and a further 38% felt that there was a growing maturity around this in the bank.

Attraction and retention of digital talent ranked relatively low, with 13% of respondents feeling that the bank was an industry leader. What was positive is that 42% recognised that there is growing maturity in the bank around this, but 34% were of the view that the bank was in the middle of the pack relative to its peers.

5.3.2.2 *Tools used to manage risks*

The feedback that was analysed from the qualitative study highlighted that the staff who are responsible for risk management in the bank needs access to tools that allow them to manage digital risks. It further revealed that the tools require improvement in order to successfully manage the risk downwards.

The lack of automated risk tools was highlighted in both the interviews and the responses from the quantitative data collection. The qualitative interviews revealed that there is room for improvement within the organisation to digitise and automate risk tools. The qualitative data from the fit for future assessment shows that the respondents feel that the bank needed to do more, 47% of the responses indicating that the bank is in the middle of the pack when compared to its peers, 30% indicated that the bank is growing in maturity in this aspect, but only 2% believed that the bank could be acknowledged as an industry leader in this area.

Similarly, the leveraging of big data, analytics and AI revealed that only 9% felt the bank was an industry leader, with 59% saying that they observe growing maturity and 24% indicating that the bank was in the middle of the pack when compared against its peers. The degree to which banks employ big data, AI and ML to assist with not only its operations but also it for risk management will determine how successful they will be in their digital transformation strategies.

The importance of big data, AI and ML have been stressed by Choi et al. (2017), Aziz and Dowling (2019) and Hassani et al. (2018).

5.3.3 *Conclusion: Proposition 2*

The digital risk assessment through the survey responses revealed that the respondents believed that the risk of a data breach or cyberattack, will increase over the next three years with 51% of respondents strongly agreeing and a further 39% agreeing. That is a collective 90% of the respondents seeing an increased risk, implying that the bank needs to accelerate its efforts in mitigating this risk by ensuring that it has the right skills and tools to manage the risks successfully through digital transformation and into the future.

There does not seem sufficient evidence to suggest that banks in South Africa are prepared to respond appropriately to risks that result from digitalisation, as skills is a growing concern and having access to the right tools to appropriately and timeously manage risk is not currently a reality.

5.4 Conclusion

The chapter discussed the findings as it relates to the literature that was reviewed in the first two chapters. This research was a mixed-method study to explore how digitalisation impacts the risk management framework in the South African Banking industry. This research report examined the impact that digitalisation has on banking and how banks subsequently respond.

Two propositions were made, that was studied by collecting data through a research questionnaire and through face-to-face interviews. The two research

i. Proposition 1: There is an increased inherent risk associated with digitalisation in banking, as digitalisation increases the impact, the probability and the velocity at which risks approach the banking industry.
ii. Proposition 2: Banks in South Africa are prepared to respond appropriately to risks that result from digitalisation, as they are sufficiently skilled and have the right tools to perform their duties.

The next and final chapter concludes the research and provides recommendations and suggestions for future research.

6 CONCLUSIONS & RECOMMENDATIONS

6.1 Introduction

This chapter integrates the findings of the two propositions that were made into the original research question and objectives from Chapter 1. The chapter concludes with recommendations and suggestions for future research.

6.2 Preparedness of banks to respond to the inherent risks of digitalisation

Rogers (2016) and Ismail et al. (2014) highlighted the need for a successful organisation of the future, to have a healthy appetite for risk in order to remain relevant and competitive.

The appropriate threshold for the organisation's risk appetite can only be determined if the bank is aware of the risks that they face through knowing the impact, likelihood and velocity that make up the inherent risk exposure of the bank.

This highlights the controls that need to be put in place by the organisation in order to manage the residual risk down to acceptable levels to remain relevant and competitive without incurring massive financial penalties or reputational risk.

6.3 Responsiveness of banks to the inherent risks of digitalisation

In an environment that shares many common characteristics as it relates to speed, appropriate tools are required to respond timeously to those risk as well.

The need for digital risk management tools and control in the domains of big data, AI and ML, is especially important and relevant for digitally transforming organisations and therefore, the risk management functions across the three lines of defence need to be digitalised as well.

This is especially important for banks, who are increasingly seeing data and the use of big data as a competitive differentiator. The increasing use of data coupled with the use of new technologies will increase the risks where the bank operates and presents its products to its customers, not only in the physical world but also in cyberspace.

6.4 Recommendations

The digitalisation of risk management in the South African banking industry should be seen as a priority for banks. Growing competition and increasing demands from customers have driven the need for banks to evolve.

Banks can no longer rely on a model that looks at only two dimensions of risk, i.e. impact and likelihood. The complexity and speed that digitalisation brings through the varying digital technologies that get introduced, requires a model that takes this into account. Risk management should be able to respond to risk and be able to advise business and members of the board with greater speed and accuracy than what they are doing today. Once the risk model has been revisited, a full risk assessment and risk maturity study need to be undertaken across the organisation. The current and future risk scenarios should be developed and the risk appetite for the organisation needs to be set at an appropriate level to enable growth, explore new opportunities and deliver on customer needs and promises.

The communication of the digital transformation strategy should be communicated throughout the organisation, with greater frequency. It is important, that at all levels of the organisation and across all the segments, business units and staff members must have a common understanding of the organisation’s strategy. Additionally, the organisational strategy should define the strategies for the supporting functions in the group, who must enable the strategic levers of the bank. This means that the digital transformation strategy of the bank should be supported by a digital risk, human resource, finance and information technology strategy to be successful. This implies a single view and purpose for the future across all three lines of defence, across all levels of staff, be it executive

and senior management, middle management or junior management and specialists.

Along with data, human resources and skills should be seen as key strategic assets of the bank. The fluidity of skills across different companies coupled with an increasing immigration trend in South Africa should be alarming for executives. The focus on retention and attraction of top digital talent should be a top priority for banks. Also, existing talent should be multi-skilled and trained in new disciplines that support the digital transformation journey and changing risk landscape.

The organisation needs to ensure that people across the organisation and three lines of defence have access to the appropriate tools to enable the digitalisation of the organisation and the risk response and mitigation actions.

6.5 Suggestions for further research

The study was a case study approach and broadening the scope to include all of the big five banks and also the new entrants in the form of Fintechs are suggested.

The research is focussed only on the South African Retail Banking industry and did not include mutual banks, investment banks or development and land banks. For future research, the study may be broadened to include all banking institutions in South Africa.

In addition, banks are diversifying their services to include insurance and telecommunications. The extent to which these organisations compete and their risk appetites could provide an interesting insight into the number of risks that bank in the future should be taking on in order to remain competitive and relevant.

Furthermore, due to increasing global expansion of South African firms, the risk associated with banks internationally will add great significance. Country risk is a direct contributor to an organisation's overall risk profile as it increases complexity, regulatory obligations and encompasses different customer needs and wants typically associated with varying cultures and beliefs.

Vulnerability as the fourth dimension of risk assessment was not researched as part of this study. This dimension has been proposed by Curtis and Carey (2012) and could provide an interesting insight into what an enhanced risk model would look like that spans over four dimensions instead of three, i.e. impact, likelihood and velocity.

It is then suggested that future research looks at broadening the scope of the study based on the number of banks observed, industry players or geographical footprint. It is also suggested that the gap between traditional risk management and digital risk management gets defined, in order to develop risk models for both inherent and residual risk, to better calculate an organisations risk appetite.

Though this research found that the current 3LoD model is working, this may drastically change based on the controls that digitalisation allows the organisation to put in place. This shift in what the traditional risk manager was expected to do and understand up to now, will drastically shift as a result of digitalisation. Future research may then also look at the skills of the future that risk managers must master in order to become efficient in managing digital risk.

REFERENCES

Aziz, S., & Dowling, M. (2019). Machine Learning and AI for Risk Management. In (pp. 33-50): Springer International Publishing.

Barapatre, V. (2019). Evolving from banking to bAInking. Retrieved from https://www.bizcommunity.com/Article/196/513/186065.html

Basel Committee on Banking Supervision (BCBS). (2006). *International Convergence of Capital Measurement and Capital Standards: A Revised Framework Comprehensive Version* Retrieved from https://www.bis.org/publ/bcbs128.pdf

Basel Committee on Banking Supervision (BCBS). (2015). *Guidelines: Corporate governance principles for banks*. Retrieved from https://www.bis.org/bcbs/publ/d328.pdf

Bernstein, P. L. (1996). *Against the gods: The remarkable story of risk*: Wiley New York.

BusinessDictionary. (Ed.) (2019). WebFinance Inc.

BusinessTech. (2017). Robots are taking over SA's finance sector in a big way. Retrieved from https://businesstech.co.za/news/banking/201356/robots-are-taking-over-sas-finance-sector-in-a-big-way/

Cairns, P. (2017, 2017-08-11). Is technology changing what banks do, or just how they do it? Retrieved from https://www.moneyweb.co.za/mymoney/is-technology-changing-what-banks-do-or-just-how-they-do-it/

Chen, H., Chiang, R. H. L., & Storey, V. C. (2012). Business Intelligence and Analytics: From Big Data to Big Impact. *MIS Quarterly, 36*(4), 1165. doi:10.2307/41703503

Choi, T. M., Chan, H. K., & Yue, X. (2017). Recent Development in Big Data Analytics for Business Operations and Risk Management. *IEEE Trans Cybern, 47*(1), 81-92. doi:10.1109/TCYB.2015.2507599

Clemente, D. (2015). *Fundamentals of cyber security*. In L. McFaul (Ed.), *Verification & Implementation: A biennial collection of analysis on international agreements for security and development* (pp. 163 - 180). Retrieved from www.vertic.org

Coetzee, J. (2018). Strategic implications of Fintech on South African retail banks. *South African Journal of Economic and management Sciences, 21*(1), 11. doi:10.4102/sajems.v21i1.2455

Collins, L. M., Schafer, J. L., & Kam, C.-M. (2001). A comparison of inclusive and restrictive strategies in modern missing data procedures. *Psychological Methods, 6*(4), 330-351. doi:10.1037/1082-989X.6.4.330

Cruz, M., Coleman, R., & Salkin, G. (1998). Modeling and measuring operational risk. *The Journal of Risk, 1*(1), 63-72. doi:10.21314/jor.1998.002

Curtis, P., & Carey, M. (2012). *Risk assessment in practice*. Retrieved from https://www.coso.org/Documents/COSO-ERM-Risk-Assessment-in-Practice-Thought-Paper-October-2012.pdf

Defense Systems Management College. (2001). *Risk Management Guide for DOD Acquisition* (4th ed.). Fort Belvoir, Virginia: Defense Acquistion University Press.

Deloitte. (2019). Managing the Digital Risks of New Business Models. Retrieved from https://deloitte.wsj.com/riskandcompliance/2018/05/07/managing-the-digital-risks-of-new-business-models/

Cybercrimes and Cybersecurity Bill, (2017).

Digital Risk Management Institute. (2019). What is Digital Risk Management? Retrieved from http://www.drminstitute.org/what-is-digital-risk-management/

Doyle, K. (2018, 2018-07-24). Pepper helps Nedbank lead in digital. Retrieved from https://www.itweb.co.za/content/lLn147myL9m7J6Aa

Edwards, J. R., & Lambert, L. S. (2007). Methods for integrating moderation and mediation: a general analytical framework using moderated path analysis. *Psychological Methods, 12*(1), 1.

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics, 5*(1). doi:10.11648/j.ajtas.20160501.11

Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. *International Journal of Information Management, 35*(2), 137-144. doi:10.1016/j.ijinfomgt.2014.10.007

Gartner. (Ed.) (2019) Gartner IT Glossary. Gartner.

Grasshoff, G., Coppola, M., Pfuhler, T., Gittfried, N., Bochtler, S., Vonhoff, V., & Wiegand, C. (2019). Global Risk 2019: Creating a More Digital, Resilient Bank. Retrieved from https://www.bcg.com/publications/2019/global-risk-creating-digital-resilient-bank.aspx

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2009). *Multivariate Data Analysis* (7th ed.). Pearson.

Härle, P., Havas, A., & Samandari, H. (2016). The future of bank risk management. 1 - 7. Retrieved from https://www.mckinsey.com/business-functions/risk/our-insights/the-future-of-bank-risk-management

Hassani, H., Huang, X., & Silva, E. (2018). Digitalisation and Big Data Mining in Banking. *Big Data and Cognitive Computing, 2*(3), 18. doi:10.3390/bdcc2030018

ICT Works. (2019). Five Problems with the Fourth Industrial Revolution. Retrieved from https://www.ictworks.org/problems-fourth-industrial-revolution/

International Organization for Standardization. (2009). ISO Guide 73:2009 Risk Management Vocabulary. In (Vol. 73:2009). Geneva, Switzerland: ISO.

International Organization for Standardization. (2018). ISO 31000 Risk management. Retrieved from https://www.iso.org/iso-31000-risk-management.html

IRMSA. (2019). *2019 Enterprise risk management benchmark survey: South Africa*. Retrieved from South Africa: https://cdn.ymaws.com/www.irmsa.org.za/resource/resmgr/2019_resources/email_resources/risk_maturity/2019_South_Africa_Risk_Matur.pdf

IRMSA. (2020). *IRMSA Risk Report: South Africa risks 2020*. Retrieved from https://files.irmsa-techlibrary.org.za/riskreport2020/files/downloads/IRMSA-Risk-Report-2020.pdf

Ismail, S., Malone, M. S., van Geest, Y., & Diamandis, P. H. (2014). *Exponential Organizations: Why new organizations are ten times better, faster and cheaper than yours (and what you need to do about it)*. New York: Diversion Books.

Khumalo, K. (2018). Nedbank launches first humanoid robot in SA at branch | IOL Business Report. Retrieved from https://www.iol.co.za/business-report/companies/nedbank-launches-first-humanoid-robot-in-sa-at-branch-13596888

Korstjens, I., & Moser, A. (2018). Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *Eur J Gen Pract, 24*(1), 120-124. doi:10.1080/13814788.2017.1375092

Kumar, M., Saumya, S., Berz, K., Le Boulay, G., Tang, T., Tripathi, S., . . . Robin, M. (2019). Banks Brace for a New Wave of Digital Disruption. Retrieved from https://www.bcg.com/publications/2019/banks-brace-new-wave-digital-disruption.aspx

Lee, G. J. (2016). *Business statistics from Scratch to Intermediate in SAS.*: Silk Route Press.

Mahajan, R., Parthasarathy, S., & Jain, V. (2018). *Managing Risk in Digital Transformation*. Retrieved from United Kingdom: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-managing-risk-in-digital-transformation-1-noexp.pdf

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., & Byers, A. H. (2011). Big data: The next frontier for innovation, competition. *Washington, DC: McKinsey Global Institute*.

Morse, J. M. (2015). Critical analysis of strategies for determining rigor in qualitative inquiry. *Qualitative health research, 25*(9), 1212-1222.

Moyo, A. (2019). Digital newcomers spark price war among SA banks. Retrieved from https://www.itweb.co.za/content/KA3WwqdlL1aqrydZ

Pyle, D. H. (1999). Bank Risk Management: Theory. In (pp. 7-14): Springer US.

Qualtrics. (2019). How to Determine the Correct Survey Sample Size. Retrieved from https://www.qualtrics.com/experience-management/research/determine-sample-size/

Quan, S. N. G., & Chiang, A. (2017). *Risk management at the speed of business*. Retrieved from https://www.pwc.com/sg/en/risk-assurance/assets/ra-sid-risk-velocity.pdf

Ramaphosa, C. (2019). *President Cyril Ramaphosa: South African Digital Economy Summit | South African Government.* Paper presented at the 1st South African Digital Economy Summit, Gallagher Convention Centre, Johannesburg.

Rogers, D. L. (2016). *The digital transformation playbook : rethink your business for the digital age*.

Rossi, C. (2017). How Behavioral Economics Can Elevate Strategic Risk Management. Retrieved from https://www.garp.org/#!/risk-intelligence/all/all/a1Z1W000003rJJE?utm_source=%20weekinrisk&utm_medium=email&utm_campaign=weekinrisk&utm_term=article1

RSA Security. (2019a). 10 Major factors affecting your digital risk profile [White Paper]. Retrieved from https://www.rsa.com/content/dam/en/white-paper/ten-major-factors-affecting-your-digital-risk-profile.pdf

RSA Security. (2019b). Introduction to Digital Risk Management | RSA. Retrieved from https://www.rsa.com/en-us/discover/digital-risk-management

RSA Security. (2019c). *RSA Digital risk report 2019*. Retrieved from https://www.rsa.com/en-us/offers/rsa-digital-risk-report-second-edition

Saunders, M., & Lewis, P. (2012). *Doing Research in Business & Management: An Essential Guide to Planning Your Project Pearson*. Harlow, Essex, England: Pearson.

Schwab, K. (2016). *The Fourth Industrial Revolution*: World Economic Forum.

South African Reserve Bank. (2018). *Bank Supervision Annual Report 2017*. Retrieved from https://www.resbank.co.za/Publications/Detail-Item-View/Pages/Publications.aspx?sarbweb=3b6aa07d-92ab-441f-b7bf-

bb7dfb1bedb4&sarblist=21b5222e-7125-4e55-bb65-56fd3333371e&sarbitem=8507

Sreedhar, S. (2018, 2018-10-08). Key strategies for effective digitalization in Banks. Retrieved from https://www.finextra.com/blogposting/16097/key-strategies-for-effective-digitalization-in-banks

Stoneburner, G. (2006). Toward a Unified Security/Safety Mode. *IEEE Computer, 39*(8), 96–97.

Sumner, M. (2009). Information Security Threats: A Comparative Analysis of Impact, Probability, and Preparedness. *Information Systems Management, 26*(1), 2-12. doi:10.1080/10580530802384639

SurveyMonkey. (2019). Sample Size Calculator: Understanding Sample Sizes | SurveyMonkey. Retrieved from https://www.surveymonkey.com/mp/sample-size-calculator/

The Centre of Excellence in Financial Services. (2019). *The impact of the fourth industrial revolution on financial services in South Africa*. Retrieved from Johannesburg: https://www.coefs.org.za/research-reports/impact-4th-industrial-revolution-south-african-financial-services-market-report/

Weichert, M. (2017). The future of payments: How FinTech players are accelerating customer-driven innovation in financial services. *Journal of Payments Strategy & Systems, 11*(1), 23-33.

Xu, M., David, J. M., & Kim, S. H. (2018). The Fourth Industrial Revolution: Opportunities and Challenges. *International Journal of Financial Research, 9*(2). doi:10.5430/ijfr.v9n2p90

APPENDICES

APPENDIX A: Participant information sheet – Web survey

Dear participant,

I am a Master of Management in Digital Business student at the University of Witwatersrand Business School. As part of fulfilment of my studies, I am required to undertake a research project. I am examining the Digitalisation of risk management in the South African banking industry. This research aims to identify preparedness of banks for digitalisation and whether or not risk strategies and business strategies are sufficiently geared for the opportunities and challenges that digitalisation brings.

Your participation in the project would add tremendous value. Your participation in completing the web-based questionnaire would be appreciated and it should not consume more than 10 minutes of your time. Your participation is voluntary and will not be remunerated.

Your response is completely confidential and anonymous. Thank you for taking the time to complete the questionnaire. Should you wish to obtain more information, you are welcome to contact me, my supervisor or the university as per the information provided below.

Kind regards,

Franco Gresse.

Student:

Name: Lambert François Gresse

Email: 2289117@students.wits.ac.za

Contact nr.: +27 82 481 7667

Supervisor:

Name: Dr. Thanti Mthanti

Email: thanti.mthanti@wits.ac.za

Contact nr.: +27 11 717 3564

APPENDIX B: Participant agreement form – Interviews

Participants in the interviews were each requested to accept a meeting request, detailing that their response is completely confidential and anonymous. That they can withdraw at any time and that they understand that their participation will anonymously form part of a research project that may be published. Acceptance of the meeting requests has been recorded.

Gresse, Franco

Subject:	Interview Request: Digital Risk Management
Location:	*Removed for confidentiality purposes*
Start:	Wed 2020/02/05 10:00
End:	Wed 2020/02/05 11:30
Recurrence:	(none)
Meeting Status:	Meeting organizer
Organizer:	Gresse, Franco
Required Attendees:	*Removed for confidentiality purposes*
Categories:	Studies

Dear *<Removed for confidentiality purposes>*,
I am a Master of Management in Digital Business student at the University of Witwatersrand Business School. As part of fulfilment of my studies, I am required to undertake a research project. I am examining the impact of digitalisation on risk management, in South African banks. This research aims to identify preparedness of banks for digitalisation and whether or not risk strategies and business strategies are sufficiently geared for the opportunities and challenges that digitalisation brings.

Your participation in the project would add tremendous value. Your participation in allowing me to interview you would be greatly appreciated and it should not consume more than 45 minutes of your time. Your participation is voluntary and will not be remunerated.

Your response is completely confidential and anonymous. You can withdraw at any time and you understand that your participation will anonymously form part of a research project that may be published.

Should you wish to obtain more information, you are welcome to contact me, my supervisor or the university as per the information provided below.

Kind regards,
Franco Gresse.

Student:
Name: Lambert François Gresse
Email: 2289117@students.wits.ac.za
Contact nr.: +27 82 481 7667

Supervisor:
Name: Dr. Thanti Mthanti
Email: thanti.mthanti@wits.ac.za
Contact nr.: +27 11 717 3564

APPENDIX C: Questionnaire – Web survey

Digitalisation of risk management in the South African banking industry v1.0

Survey Flow

Standard: Welcome (1 Question)
Block: Respondent Information (9 Questions)
Standard: A. Fit for future assessment (1 Question)
Standard: B. Perceived Inherent Risk (1 Question)
Standard: C. Digital Risk Assessment (1 Question)
Standard: D. Digital Risk Assessment (1 Question)
Standard: E. Risk Response / Risk Management (1 Question)

EndSurvey:

Page Break

Start of Block: Welcome

Q0

Dear participant,

I am a Master of Management in Digital Business student at the University of Witwatersrand Business School. As part of fulfillment of my studies, I am required to undertake a research project. I am examining the Digitalisation of risk management in the South African banking industry. This research aims to identify preparedness of banks for digitalisation and whether or not risk strategies and business strategies are sufficiently geared for the opportunities and challenges that digitalisation brings.

Your participation in the project would add tremendous value. Your participation in completing the web-based questionnaire would be appreciated and it should not consume more than 10 minutes of your time. Your participation is voluntary and will not be remunerated.

Your response is completely confidential and anonymous. Thank you for taking the time to complete the questionnaire. Should you wish to obtain more information, you are welcome to contact me, my supervisor or the university as per the information provided below.

Kind regards,

Franco Gresse.
Email: fgresse@xxxx.co.za

Supervisor Name: Dr. Thanti Mthanti
Email: thanti.mthanti@wits.ac.za

End of Block: Welcome

Start of Block: Respondent Information

Q1

In the following 9 questions, please tell me a bit more about yourself, bearing in mind that your response is completely confidential and anonymous.

Please specify your gender:

- ○ Male (1)
- ○ Female (2)
- ○ Other (3)
- ○ Prefer not to say (4)

Q2 **Please specify your age range:**

- ○ 18-24 years old (1)
- ○ 25-34 years old (2)
- ○ 35-44 years old (3)
- ○ 45-54 years old (4)
- ○ 55-64 years old (5)
- ○ 65-74 years old (6)
- ○ 75 years or older (7)

Q3 **Please select the options which best describes your employment status:**

- ○ Permanently Employed (1)
- ○ Temporarily Employed (2)
- ○ Fixed Term Contract (Self-employed / Private) (3)
- ○ Fixed Term Contract (Agency / External Company) (4)

Q4 **Please select the option which best describes your job role:**

- ○ Business or Business Support (Product, Sales, Operations, Marketing, IT, HR, Finance, etc.) (1)
- ○ Risk Management (Legal, Risk, Regulatory Risk, Fraud, etc.) (2)
- ○ Group Internal Audit (3)

Q5 **Please select the option which best describes your position:**

- ○ Specialist / Analyst (1)
- ○ Junior Management (2)
- ○ Middle Management (3)
- ○ Senior Management (non-Exco) (4)
- ○ Business Exco / Segment Exco (excluding CEO / Segment CxO) (5)
- ○ Executive (Business CEO / Segment CxO / Organisational Head / CEO) (6)

Q6 **Please indicate how long you have been employed by the bank or delivering a service to the bank as a contractor:**

- ○ < 3 years (1)
- ○ 3 - 5 years (2)
- ○ 5 - 7 years (3)
- ○ 7 - 10 years (4)
- ○ > 10 years (5)

Q7 **Please indicate your highest qualification:**

- ○ High school graduate (Matric) (1)
- ○ Some college credit, no degree (2)
- ○ Trade/technical / vocational training (3)
- ○ Professional Certification (4)
- ○ Diploma (5)
- ○ Bachelor’s Degree (6)
- ○ Honours Degree (7)
- ○ Master’s Degree / MBA (8)
- ○ Doctorate Degree / PhD (9)

Q8 **Please indicate if you are currently studying in the field of Risk Management:**

- ○ Yes (1)
- ○ No (2)
- ○ Planning to start (3)
- ○ Recently completed (4)

Q9 **Please indicate if you are currently studying in the field of Digital Business / Digital Transformation:**

- ○ Yes (1)
- ○ No (2)
- ○ Planning to start (3)
- ○ Recently completed (4)

End of Block: Respondent Information

Start of Block: A. Fit for future assessment

Q10

The following sections (A to E) will be quick to complete. Please answer as accurately as possible.

A. Fit for future assessment

Rate the following as you perceive it **relative to the organisation's competitors**:

	Disadvantaged (1)	Experimental (2)	Middle of the pack (3)	Growing maturity (4)	Industry leadership (5)
We drive to achieve scale in the organisation relative to its competitors (1)	○	○	○	○	○
Digitise end-to-end customer journey (2)	○	○	○	○	○
Leverage big data, analytics & AI (3)	○	○	○	○	○

	Disadvantaged (1)	Experimental (2)	Middle of the pack (3)	Growing maturity (4)	Industry leadership (5)
Pursue partnerships to increase capabilities and scale (4)	○	○	○	○	○
Adopt new ways of working (5)	○	○	○	○	○
Attract and retain digital talent (6)	○	○	○	○	○
Simplify technology and data infrastructure (7)	○	○	○	○	○

	Disadvantaged (1)	Experimental (2)	Middle of the pack (3)	Growing maturity (4)	Industry leadership (5)
Ensure cybersecurity resilience (8)	○	○	○	○	○
Risk tools are digitised (9)	○	○	○	○	○
We regularly train, upskill and invest in learning & development of digital technology (10)	○	○	○	○	○

End of Block: A. Fit for future assessment

Start of Block: B. Perceived Inherent Risk

Q11 *B. Perceived Inherent Risk*

Please select the option which best indicates the degree to which you agree or disagree with the statement:

	Strongly disagree (1)	Somewhat disagree (2)	Neither agree nor disagree (3)	Somewhat agree (4)	Strongly agree (5)
IMPACT: Digital transformation will result in an increase in risk impact (1)	○	○	○	○	○
LIKELIHOOD: Digital transformation will result in a greater probability that risk will materialise (2)	○	○	○	○	○
VELOCITY: Digital transformation will result in an increase in the speed at which risk approach the bank (3)	○	○	○	○	○

	Strongly disagree (1)	Somewhat disagree (2)	Neither agree nor disagree (3)	Somewhat agree (4)	Strongly agree (5)
CONTROLS: Digital transformation will allow us to better respond to risks in the future (4)	○	○	○	○	○

End of Block: B. Perceived Inherent Risk

Start of Block: C. Digital Risk Assessment

Q12 *C. Digital Risk Assessment*

Please select an option which best describes or completes the statement:

	Very Low / Minimal / Small (1)	Low (2)	Medium / Neutral (3)	High / Large (4)	Very High / Complex / Extra Large (5)
The organisation needs to comply with a great deal of local, international and industry regulations (1)	○	○	○	○	○
The organisation is highly dependant on third parties and partnerships (2)	○	○	○	○	○

	Very Low / Minimal / Small (1)	Low (2)	Medium / Neutral (3)	High / Large (4)	Very High / Complex / Extra Large (5)
The degree to which the business requires business resilience, disaster management and business continuity management capabilities (3)	○	○	○	○	○

	Very Low / Minimal / Small (1)	Low (2)	Medium / Neutral (3)	High / Large (4)	Very High / Complex / Extra Large (5)
I rate the complexity of the overall organisation as _____, as it relates to our business model, strategy, geographic scope and competitive environment. (4)	○	○	○	○	○

	Very Low / Minimal / Small (1)	Low (2)	Medium / Neutral (3)	High / Large (4)	Very High / Complex / Extra Large (5)
I rate the technical complexity of the overall organisation as _____, as it relates to our data sets, IT systems and applications. (5)	○	○	○	○	○

End of Block: C. Digital Risk Assessment

Start of Block: D. Digital Risk Assessment

Q13 *D. Digital Risk Assessment*

Please select the option which best indicates the degree to which you agree or disagree with the statement:

	Strongly disagree (1)	Somewhat disagree (2)	Neither agree nor disagree (3)	Somewhat agree (4)	Strongly agree (5)
I feel the risks have increased since the introduction of digital transformation (1)	○	○	○	○	○
I feel the risks that digitalisation introduces outweighs the benefits (2)	○	○	○	○	○

	Strongly disagree (1)	Somewhat disagree (2)	Neither agree nor disagree (3)	Somewhat agree (4)	Strongly agree (5)
The organisation will face serious disruption & threats over the next three years (increased competition) (3)	○	○	○	○	○
I feel the risk of a cyberattack or data breach has increased over the past three years (4)	○	○	○	○	○

	Strongly disagree (1)	Somewhat disagree (2)	Neither agree nor disagree (3)	Somewhat agree (4)	Strongly agree (5)
I feel more comfortable with processes being automated, i.e. using robotics and artificial intelligence to conduct business activities (5)	○	○	○	○	○
I feel comfortable that risk functions and capabilities are fully automated (6)	○	○	○	○	○

End of Block: D. Digital Risk Assessment

Start of Block: E. Risk Response / Risk Management

Q18

E. Risk Response / Risk Management

Please select the option which best indicates the degree to which you agree or disagree with the statement:

	Strongly disagree (1)	Somewhat disagree (2)	Neither agree nor disagree (3)	Somewhat agree (4)	Strongly agree (5)

"The bank operates under an independent 3 Line of defence model, i.e.: i. First line of defence: The business line, i.e. Marketing, Operations, Sales, Product Management, etc; ii. Second line of defence: An independent risk management function including legal, risk, regulatory and fraud risk management; iii. Third line of defence: An independent	○	○	○	○	○

	Strongly disagree (1)	Somewhat disagree (2)	Neither agree nor disagree (3)	Somewhat agree (4)	Strongly agree (5)
internal audit function. " (1)					
The workforce is mobile and able to work remotely without hampering business operations or productivity (2)	○	○	○	○	○
We have a modern compliance programme that is geared for digital transformation and digital risks (3)	○	○	○	○	○

	Strongly disagree (1)	Somewhat disagree (2)	Neither agree nor disagree (3)	Somewhat agree (4)	Strongly agree (5)
We have an evolved data governance and privacy programme (e.g. GDPR & POPI) (4)	○	○	○	○	○
Risk evaluation of new processes are fully automated (5)	○	○	○	○	○
The digital business is safeguarded against a range of digital threats (6)	○	○	○	○	○

	Strongly disagree (1)	Somewhat disagree (2)	Neither agree nor disagree (3)	Somewhat agree (4)	Strongly agree (5)
Our technologies are moving towards cloud based and other diversified technology architectures (7)	○	○	○	○	○
The organisation is capable of safeguarding and securing the cloud infrastructure (8)	○	○	○	○	○

	Strongly disagree (1)	Somewhat disagree (2)	Neither agree nor disagree (3)	Somewhat agree (4)	Strongly agree (5)
I am confident that my organisation can protect our customers' personal data (9)	○	○	○	○	○
The digitalisation strategy has been communicated throughout the organisation (10)	○	○	○	○	○
Senior management supports the risk function throughout the digital transformation journey (11)	○	○	○	○	○

	Strongly disagree (1)	Somewhat disagree (2)	Neither agree nor disagree (3)	Somewhat agree (4)	Strongly agree (5)
I am confident that the business is able to adequately recover when a risk materialises through the use of digital technologies and skills (12)	○	○	○	○	○
We have the skills and capabilities to deliver products and services that is required to remain competitive in the future (13)	○	○	○	○	○

End of Block: E. Risk Response / Risk Management

APPENDIX D: Questionnaire – Interviews

Question #	Research Question
A. Introduction: Digital Transformation, platforms, digitisation and competition	
A1	Would you say that the bank has taken the lead as one of the traditional banks in terms of digitalisation / digital transformation? What would your reasons be for saying so?
A2	In your opinion, has the bank fully entrenched itself into platform thinking? If so why?
A3	Has the competitive landscape changed dramatically, and do you perceive the bank to be under threat by especially non-traditional banks, such as Tyme Bank and Discovery Bank? If so, why do you say so?
A4	Do you believe that digital transformation is essential towards steering the bank in a sustainable strategic direction? Please validate your answer.

Question #	Research Question
A5	Has senior management communicated the transformation strategy throughout the organisation?
B. Proposition 1: There is an increased inherent risk associated with digitalisation in banking, as digitalisation increases the impact, the probability, and the velocity at which risks approach the banking industry.	
B1	Do you believe that the inherent risk associated with digitalisation will change (increase / decrease)? If so, why? Please elaborate.
B1a	a. Would you say that the probability of a risk event materialising would increase or decrease with digitalisation? Please elaborate.
B1b	b. Would you say that digitalisation causes the inherent risk to increase in terms of impact or decrease? Please elaborate.
B1c	c. Would you say that the velocity (speed of onset) would increase or decrease with digitalisation? Please elaborate.

Question #	Research Question
B1d	d. Is the bank currently measuring risk by including Velocity in its Inherent and Residual Risk calculations? If not, is it being considered?
C. Proposition 2: Banks in South Africa are prepared to respond appropriately to risks that result from digitalisation, as they are sufficiently skilled and have the right tools to perform their duties.	
C1	Do you believe that the Three Lines of Defence model is crucial towards managing risk, both traditionally and going forward as the bank goes through the digital transformation process?
C1a	a. In your opinion, are digital skills embedded across the 3LoD crucial for digital transformation of the organisation?
C1b	b. In your opinion, is digital skills across the 3LoD crucial for future risk management of the organisation?
C1c	c. What top three skills do you think is important and why?

Question #	Research Question
C1d	d. What is the top three biggest risk that the bank faces in terms of skills during the 4th Industrial Revolution and during its digital transformation journey?
C1e	e. Based on this, do you think that the attraction and retention of digital skills and talent are receiving enough attention / strategic focus? Why?
C2	Do staff who are responsible for risk management have adequate access to tools to manage risk inherent in digital transformation but also to manage digital risks?
C3	Are risk tools / processes sufficiently digitised / automated? Why?
D. Risk Response / Risk Management	
D1	In terms of Cybersecurity, how would you describe the bank's ability to monitor, detect and respond to threats? Why?

Question #	Research Question
D2	How would you describe the bank's ability in terms of crisis management, business continuity and disaster recovery?
D3	How would you describe the bank's ability to comply with Data governance and Data Privacy laws?
D4	Are you confident that the bank can safeguard and protect its customers' data?
D5	How would you describe the bank's ability to secure cloud infrastructure?
D6	Do you feel that the bank manages third party risk sufficiently? Why?
D7	How would you describe the bank's ability to securely manage user access and identities?
D8	Do you think that the bank is mature in managing the digitisation of manual business processes? Why?

Question #	Research Question
D9	Do you think that the bank runs a modern compliance programme and are able to respond to regulatory changes sufficiently?
D10	Does senior management support the risk management function?
D11	Do you believe that the bank has successfully embraced the concept of a mobile workforce?

APPENDIX E: Consistency Matrix

Figure 48: Consistency Matrix

Research problem: The impact of digitalisation on risk management in banking					
Objective #	**Research Objective**	**Proposition**	**Data source & type**	**Analysis Method**	**Literature Review**
1.	Are banks prepared for the inherent risk associated with digitalisation?	Proposition 1	Qualitative (interviews) and quantitative (questionnaires)	Qualitative: Thematic analysis Quantitative: Descriptive statistics and statistical analysis	Quan and Chiang (2017) RSA Security (2019c) Chen et al. (2012) Gandomi and Haider (2015) Clemente (2015) Rogers (2016)

Research problem: The impact of digitalisation on risk management in banking					
Objective #	**Research Objective**	**Proposition**	**Data source & type**	**Analysis Method**	**Literature Review**
					Ismail et al. (2014) Weichert (2017)
2.	Are banks ready to respond to risks associated with digitalisation?	Proposition 2	Qualitative (interviews) and quantitative (questionnaires)	Qualitative: Thematic analysis Quantitative: Descriptive statistics and statistical analysis	Basel Committee on Banking Supervision (BCBS) (2015) IRMSA (2020) Clemente (2015) Choi et al. (2017) Aziz and Dowling (2019) Hassani et al. (2018)

APPENDIX F: Ethics Approval Letter

UNIVERSITY OF THE WITWATERSRAND JOHANNESBURG

SCHOOL OF GRADUATE SCHOOL OF BUSINESS ADMINISTRATION ETHICS COMMITTEE
CONSTITUTED UNDER THE UNIVERSITY HUMAN RESEARCH ETHICS COMMITTEE (NON-MEDICAL)

CLEARANCE CERTIFICATE	**PROTOCOL NUMBER: WBS/BA2289117/191**
PROJECT TITLE	Digitalisation of risk management in the South African banking industry: A case study of a major South African bank
INVESTIGATOR	Mr. Lambert Gresse
SCHOOL/DEPARTMENT OF INVESTIGATOR	MM (Digital Business)
DATE CONSIDERED	31 October 2019
DECISION OF THE COMMITTEE	Approved unconditionally
RISK LEVEL	LOW RISK
EXPIRY DATE	28 FEBRUARY 2021

ISSUE DATE OF CERTIFICATE 17 February 2020

CHAIRPERSON _____
(Dr MDJ Matshabaphala)

cc: Supervisor: Dr. Mthanti

DECLARATION OF INVESTIGATOR

To be completed in duplicate and **ONE COPY** returned to the Chairperson of the School/Department ethics committee.

I fully understand the conditions under which I am are authorized to carry out the abovementioned research and I guarantee to ensure compliance with these conditions. Should any departure to be contemplated from the research procedure as approved I/we undertake to resubmit the protocol to the Committee.

_____ 18 / 02 / 2020

Signature **Date**

PLEASE QUOTE THE PROTOCOL NUMBER ON ALL ENQUIRIES

APPENDIX G: Organisation – Request for Approval

Permission letter drafted to request approval to conduct research in the organisation.

08 October 2019

Att: *<removed for confidentiality>*

RE: Permission to conduct a research study in *<removed for confidentiality>*

The purpose of this letter is to request permission to conduct a research study within *<removed for confidentiality>* as part of my academic qualification **Masters in Digital Business** at Wits Business School, University of Witwatersrand.

My research paper is entitled **Digitalisation of risk management in the South African banking industry: A case study of a major South African bank.**

My study seeks to evaluate digital transformation in a retail banks and the impact of digitalisation on the risk management function, with particular focus on Operational Risk management. The purpose of the study is to investigate digital transformation within *<removed for confidentiality>* and its risk management function, as it is one of the largest banks in the country.

It is against this background that I hereby request the permission to conduct the study.

This study will receive approval from the Research Ethics Committee of the Graduate School of Business Administration, at the University of Witwatersrand.

Please note the following:

- This study will involve individual by interviews with senior leaders. As such names will not appear in the findings and the answers are given will be treated as strictly confidential. Moreover, participants cannot be identified in person based on the answers they provided.
- Data will also be collected in the form of web-based questionnaires. These will be distributed to the 3LoD across the organisation *<removed for confidentiality>* with the aim of collecting information from middle to senior managers across the organisation. Participants cannot be identified in person based on the answers they provided.
- Identified participants may choose not to participate and may also stop participating at any time.
- The name of the organisation will not be included in the final report. The final report will refer to a traditional bank or a large bank institution.
- Any sensitive information provided by the participants/respondents regarding the Bank's specific processes or strategies will treated as confidential and will not be published in the final report.
- The *<removed for confidentiality>* data protection and confidentiality requirements will be adhered to.
- All the data collected will be anonymised and kept confidential.
- The final report will be published in the Wits library and online repository.
- The results of the study will be used for academic purposes only and may be published in an academic journal. We will provide the company with a summary of the findings on request.
- Please contact me if you have any questions or comments regarding the study.

Regards,

Franco Gresse: *<removed for confidentiality>*

<removed for confidentiality>

APPENDIX H: Organisation Approval Letter

The letter has been obtained and provided to the research supervisor and ethics committee. The has requested to remain anonymous.