

Artificial Intelligence-driven transformation of risk management function in the South African Telecommunications Industry

By

Nitesh Ramatar

**A research 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, 2022

**Supervisor:
Dr Manessah Alagbaoso**

June 2022

Wits Business School

ABSTRACT

Current Artificial Intelligence (AI) solutions focus on improving business operational processes and specific applications within the risk management fraternity. AI enables organisations to accelerate processes rapidly. However, this fast pace introduces new risk exposures that require proactive risk management. Therefore, this study explored whether AI should be utilised within the risk function of a telecommunications company, to make the function proactive.

The research adopted an exploratory approach that involved conducting face-to-face interviews with risk management professionals within the telecommunications environment. The respondents' feedback was consolidated to identify and analyse findings.

Findings noted that risk functions should adopt AI to help them transition from a reactive to a proactive function. However, key challenges, such as budget constraints, poor stakeholder buy-in, and limited access to AI skills and appropriate use cases, prevent risk functions from adopting AI. Establishing change management initiatives is recommended to create a culture that can overcome these challenges.

KEYWORDS

Artificial Intelligence, Automation, Digital transformation, Transformation, Risk management, Risk function, Telecommunications industry, Telecommunications company, Technology company

DECLARATION

I, Nitesh Ramatar, 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 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: Nitesh Ramatar

Signature: 

Signed at: Paulshof

DEDICATION

The research is dedicated to the risk management fraternity and professionals within the risk management function.

ACKNOWLEDGEMENTS

I would like to take this opportunity to acknowledge my supervisor, Dr Manessah Alagbaoso, who guided me throughout the research process and challenged me to push myself. Your guidance and support are very much appreciated. I thank you.

My thanks go to the lecturers and staff at Wits Business School and especially Prof. Gregory Lee and Prof. Brian Armstrong.

To my employer, I thank you for granting me time to focus on my research.

To all participants who contributed towards the research, I thank you for your participation and support.

Lastly, I would like to thank my wife for encouraging me to pursue my studies and for all her support during this journey.

Table of Contents

ABSTRACT	ii
DECLARATION	iv
DEDICATION	v
ACKNOWLEDGEMENTS	vi
LIST OF FIGURES	xi
LIST OF TABLES	xi
LIST OF ABBREVIATIONS AND ACRONYMS	xii
Chapter 1: Introduction.....	1
1.1 Purpose of the study	1
1.2 Background of the study	1
1.3 Research problem.....	2
1.4 Research objectives.....	3
1.4.1 Main objective	3
1.4.2 Sub-objective 1	3
1.4.3 Sub-objective 2	3
1.5 Significance of the study	3
1.6 Delimitations of the study	4
1.7 Definition of terms	4
1.8 Assumptions.....	5
1.9 Chapter outline.....	6
Chapter 2: Literature Review.....	7
2.1 Introduction	7
2.2 Theory base	7
2.2.1 Theoretical framework	8
2.2.2 Overview of Artificial Intelligence	9
2.2.3 Risk management.....	10

2.2.4 Global technology, media and telecommunications industry key risks	11
2.2.5 Relationship between Artificial Intelligence and risk management.....	12
2.3 Challenges associated with Artificial Intelligence implementations	15
2.4 Organising framework	16
2.5 Conclusion of literature review	16
Chapter 3: Research Methodology	18
3.1 Research approach.....	18
3.2 Research design	18
3.3 Data-collection methods.....	18
3.4 Population	19
3.5 Sampling	19
3.6 The research instrument	20
3.7 Procedure of data collection.....	20
3.8 Data analysis and interpretation.....	20
3.9 Limitations of the study	20
3.10 Transferability, credibility, dependability and confirmability.....	20
3.10.1 Transferability	20
3.10.2 Credibility	21
3.10.3 Dependability	21
3.10.4 Confirmability	21
3.11 Demographic profile of participants.....	21
3.12 Ethical considerations	21
3.13 Summary.....	22
Chapter 4: Presentation of Findings.....	23
4.1 Introduction	23
4.1.1 Participant profile –risk management role.....	23
4.1.2 Outcomes of thematic analysis	24

4.2 Findings pertaining to Proposition 1: The increased adoption of digital technologies within the telecommunications industry in South Africa necessitates the integration of AI into the risk management function	25
4.2.1 The ability of risk function to provide business with adequate risk assurance	25
4.2.2 Risk function's ability to adopt technology at the same rate as business..	28
4.2.3 Artificial Intelligence initiatives used and their effectiveness	31
4.2.4 Current nature of the risk function.....	33
4.3 Findings pertaining to Proposition 2: AI adoption has the ability to accelerate risk management processes to proactively manage exposure.....	36
4.3.1 The ability of Artificial Intelligence initiatives to improve risk response times for better risk exposure management	36
4.3.2 Criteria for identifying appropriate risk management processes for Artificial Intelligence adoption.....	37
4.3.3 Risk management processes enabled with Artificial Intelligence that would ensure relevant risk management.....	40
4.3.4 Ideal use cases where Artificial Intelligence could be integrated for better risk exposure management	42
4.3.5 Respondent experiences regarding the impact of Artificial Intelligence on the risk function	45
4.4 Findings pertaining to Proposition 3: The implementation of AI solutions within a risk function requires an understanding of AI	47
4.4.1 Level of understanding of Artificial Intelligence	48
4.4.2 Challenges in implementing Artificial Intelligence solutions and ways of mitigating these challenges	50
Chapter 5: Discussion of the Findings.....	58
5.1 Introduction	58
5.2 Proposition 1: The increased adoption of digital technologies within the telecommunications industry in South Africa necessitates the integration of AI into the risk management function	58

5.2.1 Risk management support.....	58
5.2.2 Risk management technology adoption.....	59
5.2.3 Nature of risk management intervention – proactive vs reactive.....	60
5.3 Proposition 2 – AI adoption has the ability to accelerate risk management processes to proactively manage exposure.....	61
5.3.1 Impact of Artificial Intelligence initiatives on risk management	61
5.3.2 Criteria for identifying risk processes for Artificial Intelligence adoption....	62
5.3.3 Use cases for Artificial Intelligence adoption.....	62
5.3.4 Impact of Artificial Intelligence within the risk function	63
5.4 Proposition 3: The implementation of AI solutions within a risk function requires an understanding of AI	63
5.4.1 Understanding of Artificial Intelligence within the risk function.....	64
5.4.2 Artificial Intelligence implementation challenges.....	64
Chapter 6: Conclusions and Recommendations.....	67
6.1 Introduction	67
6.2 Conclusions pertaining to the main research objective	67
6.3 Conclusions pertaining to Research sub-objective 1.....	68
6.4 Conclusions pertaining to Research sub-objective 2.....	69
6.5 Recommendations	70
6.6 Contribution of study	71
6.7 Suggestions for further research.....	72
References.....	73
APPENDIX A: Participant information sheet for interviews	76
APPENDIX B: Consistency matrix	77
APPENDIX C: Interview guide	81
APPENDIX D: Ethics approval	83

LIST OF FIGURES

Figure 1: ISO 31 000 Risk Management Process	8
Figure 2: Top risks for 2021 and 2030 – Technology, media and telecommunications industry perspectives (Protiviti, 2021).....	12
Figure 3: Organising framework	16
Figure 4.1: Risk management support provided to business.....	26
Figure 4.2: Awareness of whether AI is being used within the risk function	31
Figure 4.3: Nature of risk management function	34
Figure 4.4: Criteria to identify risk processes for AI integration	38
Figure 4.5: Understanding of AI – good.....	48
Figure 4.6: Understanding of AI – familiar	49
Figure 4.7: Understanding of AI – limited	50

LIST OF TABLES

Table 1: Codes and themes generated during the thematic analysis	24
--	----

LIST OF ABBREVIATIONS AND ACRONYMS

AI: Artificial Intelligence

FERMA: Federation of European Risk Management Associations

HBR: Harvard Business Review

IoT: Internet of Things

IRMSA: Institute of Risk Management South Africa

ISO: International Organization for Standardization

IT: Information Technology

RPA: Robotics Process Automation

Telco: Traditional Telecommunications Company

Techco: Technology Company

UP: University of Pretoria

4IR: Fourth Industrial Revolution

Chapter 1: Introduction

1.1 Purpose of the study

This research focuses on understanding how Artificial Intelligence (AI) can be utilised to transform a risk function into a proactive function from a South African telecommunications perspective.

1.2 Background of the study

AI solutions have been deployed in organisations to improve operational processes, increase experience and derive insights at a much faster pace (Lee et al., 2020). Organisations that have been able to leverage AI capabilities successfully have been able to gain efficiencies that have given them a competitive advantage (Lee et al., 2020).

One such example is Vodacom South Africa. Vodacom has implemented a product called Airtime Advance, which allows customers to obtain an advance on airtime and pay after one month. The product is supported by big data and AI that analyses customer behaviour and prescribes an appropriate airtime advance value. Traditionally the delivery of a similar product would be manual in nature and time-consuming. However, the adoption of AI and big data has made the product successful and allowed Vodacom to gain a competitive advantage against other industry peers.

The implementation of AI in business processes has enabled organisations to accelerate processes and increase service delivery at an amazingly fast pace. However, this fast pace introduces new risk exposures to an organisation, which requires its risk management function to enhance its capabilities to adequately support the organisation.

Present studies have focused on the adoption of AI applications within services that contain an element of risk, such as credit risk, market risk and cyber-security monitoring (Aziz & Dowling, 2018). The current study seeks to understand how AI can be adopted within the actual risk management function and supplementary processes.

1.3 Research problem

The Fourth Industrial Revolution (4IR) has brought about many technological advancements that have allowed businesses to transform their operating models from traditional brick-and-mortar operations to digitally empowered operations. One such technology is AI.

According to Lee et al. (2020), financial services organisations are implementing AI solutions to create operational efficiencies, improve customer experience and derive insights (Lee et al., 2020).

In the field of risk management, research performed by Aziz and Dowling (2018) from the Rennes Business Schools in France identified the following key AI applications for risk management: credit risk, market risk, operational risk and regulatory risk (Aziz & Dowling, 2018). Aziz and Dowling's (2018) study found that organisations are investing in AI solutions to automate routine tasks and create efficiencies. One such example is the compliance division within the Spanish bank BBVA (Aziz & Dowling, 2018).

However, the integration of AI technologies into risk management processes has been slow (Lee et al., 2020). According to Aziz and Dowling (2018), a risk function faces challenges related to the availability of data, transparency and ethics around the usage of digital tools such as AI (Aziz & Dowling, 2018). Owing to these challenges, risk management decision making has been predominantly subjective in nature and needs to transition towards data-driven decision making, which is systematic in nature (FERMA, 2019).

The Institute of Risk Management South Africa's (IRMSA) 2021 survey revealed that there is a demand for risk functions to transition from a reactive function to a more proactive function, owing to the increase in risk complexity and volume (IRMSA, 2021).

Since there is limited research available related to the integration of AI into risk management functions from a South African telecommunications' perspective, the research outlined in this report aims to understand how AI technologies can be used to transform risk functions within the telecommunications industry in South Africa.

1.4 Research objectives

1.4.1 Main objective

The main objective of this study is to examine the effect of AI technologies on a risk function, and their ability to transform the risk function into a proactive function within the South African telecommunications industry.

As part of the main objective, the following sub-objectives are defined.

1.4.2 Sub-objective 1

To understand what risk applications AI can be integrated into.

1.4.3 Sub-objective 2

To investigate the barriers surrounding the adoption of AI technologies within a risk function.

1.5 Significance of the study

The rapid development of AI has created multiple use cases for AI adoption and opportunities to improve business processes.

The literature review performed as part of the current study revealed that much of the research in this area has focused on the implementation of AI to assist with managing the risk associated with specific business processes from a financial institutional perspective.

Research by Chandrinos et al. (2018) revealed that the implementation of AI to manage risk on trading portfolios successfully prevented trading portfolios from accruing losses. Aziz and Dowling (2018) investigated the implementation of AI in credit risk, market risk, operational risk and regulatory risk.

An article by Biolcheva published in the Bulgarian Trakia Journal of Sciences highlighted that risk management is rule based. With the availability of big data and sophisticated algorithms, this creates the opportunity to integrate AI into risk management processes to make these processes more proactive and able to respond in real time. However, the actual applications of AI in risk management were not explored (Biolcheva, 2020).

A key theme that arose from the literature review concerned how the topic of risk can provide real-time value to processes and enable them to keep up with the speed of business transformation.

In South Africa there is a need for risk functions to adopt a more proactive capability (IRMSA, 2021).

The significance of this study is that it investigates the barriers facing AI implementation in risk management and the identification of appropriate risk management applications of AI. The study also aims to provide suggestions for how South African telecommunications organisations can adopt AI to transform existing risk management functions.

1.6 Delimitations of the study

The study is aimed at risk management functions within telecommunications organisations within South Africa and excludes such organisations' international footprint.

The study focuses on the risk management function and does not include external risk types such as market and environmental risk.

1.7 Definition of terms

The key terms used in this study are defined below.

Artificial Intelligence: “Artificial intelligence leverages computers and machines to mimic the problem-solving and decision-making capabilities of the human mind” (IBM Cloud Education, 2020).

Big data: “is data that contains greater variety, arriving in increasing volumes and with more velocity” (Oracle, 2020). Greater variety relates to structured and unstructured data while data velocity refers to the speed at which data is generated.

Digital transformation: “Digital transformation is the process of using digital technologies to create new — or modify existing — business processes, culture, and

customer experiences to meet changing business and market requirements. This reimagining of business in the digital age is digital transformation” (Salesforce, 2021).

Control: A control can be considered a “measure that is modifying risk” (ISO, 2009).

Machine learning: “Machine learning is an application of artificial intelligence (AI) that provides systems the ability to automatically learn and improve from experience without being explicitly programmed. Machine learning focuses on the development of computer programs that can access data and use it to learn for themselves” (expert.ai, 2020).

Deep learning: is an aspect of machine learning that has the ability to teach itself while performing activities with even greater precision than machine learning (IBM Cloud Education, 2020).

Monitoring: Monitoring consists of “continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected” (ISO, 2009).

Risk: Risk is the “effect of uncertainty on objectives” (ISO, 2009).

Risk management: This involves “coordinated activities to direct and control an organization with regard to risk” (ISO, 2009).

Risk management process: This is the “systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk” (ISO, 2009).

1.8 Assumptions

This study makes the following assumptions:

- Participants have a basic understanding of business transformation and AI.
- Participants have had exposure to risk management operations or processes.
- Risk functions adopt a common risk management methodology.

1.9 Chapter outline

Chapter 1: provides an overall view of the study, beginning with the purpose of the study and the background to the study. It positions the research problem and key objectives of the study and outlines the significance of the study and its delimitations and assumptions. It also defines the key terms used in the study.

Chapter 2: presents a review of literature on the topics of AI, risk management, applications of AI to risk management and challenges associated with implementing these applications. On the basis of the literature reviewed, three research propositions are drawn up and these are presented at the end of the chapter.

Chapter 3: outlines the research methodology that was used to conduct the study. It discusses the research approach and design; the study population, sample and sampling method; the data-collection instrument and procedures; and the methods used to analyse the data. Finally, it describes the limitations of the study and the steps taken to ensure the trustworthiness of the study.

Chapter 4: presents the findings of the study. It begins with the participant profile in terms of their risk management role. The findings are then set out in line with the propositions drawn up for the study.

Chapter 5: presents a discussion of the findings structured in accordance with the study propositions.

Chapter 6: sets out the conclusions reached by the study in relation to the research objectives presented in Chapter 1 and the propositions from Chapter 2. From the conclusions, recommendations are made for industry practitioners and suggestions made for further research.

Chapter 2: Literature Review

2.1 Introduction

AI is a set of technologies or programs that enable machines to become more intelligent and imitate certain human tasks or capabilities to analyse, continuously learn to self-improve and act (UP, 2018). According to McKinsey (2017), AI will be one of the key technologies to drive digital disruption (McKinsey & Company, 2017). Early adopters of AI such as Amazon, Facebook, Google, Uber and Takealot have been able to leap ahead of competitors and realise benefits.

Although many of the current implementations of AI have focused on transforming core business processes, there has been some adoption of AI into business support processes, such as risk management. However, the pace of adoption of AI for support processes lags behind its use in core business transformation.

To understand AI adoption in support business functions such as the risk management function, the literature review presented in this chapter focuses on the relationship between AI and risk management. The review provides an analysis of what AI is, the types of AI, AI applications within risk functions and current challenges associated with the implementation of AI.

The literature reviewed consisted of academic journals, articles, whitepapers and conference proceedings. In addition, related government documents were included in the review.

The insights from the literature review guided the articulation of appropriate propositions at the end of the review, which are aimed at addressing the research objectives. These were deemed to provide an adequate base for executing the current study.

2.2 Theory base

This section presents the theoretical basis for the study, beginning with the theoretical framework chosen as the foundation of the study. To understand how this framework can be applied to risks that relate to AI, the concept of AI is explored, the risk

management process outlined, key telecommunications industry risks identified and the relationship between AI and risk management described.

2.2.1 Theoretical framework

The theoretical framework for the research study is based on the International Organization for Standardization 31 000 (ISO 31 000) framework of risk management. ISO 31 000 (ISO, 2009) states that the implementation of risk management enables an organisation to improve risk processes, risk governance and the proactive management of risk. Figure 1 presents the ISO 31 000 diagrammatic summary of the risk management process.

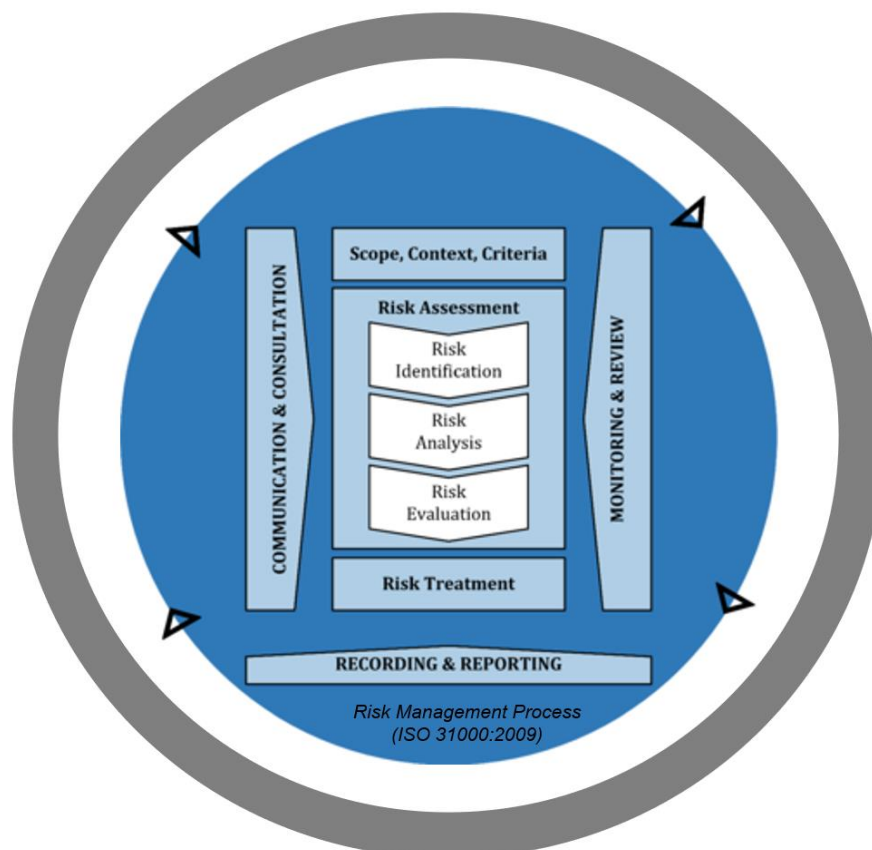


Figure 1: ISO 31 000 Risk Management Process (adapted from International Organization for Standardization 31 000)

The current study used this theory as the base for understanding the effect of AI technologies on the broader risk management function of the telecommunications industry in South Africa.

2.2.2 Overview of Artificial Intelligence

As mentioned in the introduction to this chapter, AI can be defined as technologies or programs that enable machines to imitate certain human tasks or capabilities to analyse, learn to self-improve continuously and act (UP, 2018). In all these functions, AI seeks to identify and analyse patterns to make decisions (UP, 2018).

Machine learning is programmed to learn by itself and has the ability to learn continuously from the processing of more data, to reprogram itself to perform tasks more optimally (IBM Cloud Education, 2020).

AI contains machine and deep learning concepts.

According to the Harvard Business Review (HBR), AI supports the three key business needs of automating processes, gaining cognitive insights, and cognitively engaging employees and customers (HBR, 2018).

- Process automation involves the usage of robotics process automation (RPA) to digitise physical tasks (HBR, 2018).
- Cognitive insight is the process of utilising algorithms to analyse large volumes of data to identify patterns for interpretation (HBR, 2018).
- Cognitive employee and customer engagement involve the implementation of natural language processing technologies to provide digital engagement through chatbots and intelligent agents (IBM Cloud Education, 2020).

According to McKinsey (2017), for AI to be successfully implemented, key factors such as appropriate use cases, data ecosystems, relevant infrastructure, workflow integration and an open organisational culture are required (McKinsey & Company, 2017).

The University of Pretoria (UP), in a report entitled *Artificial Intelligence for Africa*, indicates that AI growth is driven by the availability of digitised data, access to significant computer-processing power and the lower costs associated with data storage (UP, 2018). The growth of AI will improve productivity at the same time as improving output (UP, 2018).

The HBR conducted a survey in 2018 focusing on the business benefits of AI, with responses received from 250 executives. Respondents cited the following key

benefits: enhancement of product performance and functions; improved decision making; development of new products; and optimisation of processes (HBR, 2018).

Successful application of AI technologies can propel organisations forward to redefine their processing models while providing them with a competitive edge against industry peers. According to Lee et al. (2020), financial services organisations are in the process of exploring how to leverage AI technologies to reduce costs and retain their competitive edge (Lee et al., 2020).

Forbes notes that AI transformation should not be viewed as a technology implementation and that it is vital for businesses to have an understanding of AI capabilities and the value that AI offers (Forbes, 2021). Business should have knowledge of what AI solutions are and not necessarily technical knowledge (Forbes, 2021). It is important to understand automation, machine learning and deep concepts to be able to identify potential AI solution opportunities (Forbes, 2021).

2.2.3 Risk management

The management of risk concerns the coordination and control of the risks facing an organisation (ISO, 2009). Risk management is underpinned by a robust assessment approach to systematically establish risk context, assess risks to determine treatment options, and continuously review and monitor risks, for risk mitigation and reporting (ISO, 2009).

According to the ISO 31 000, risk management is the application of the risk management process. This process consists of the following stages (as outlined in Figure 1 above):

Risk identification involves the identification of positive or negative risks that may impact objectives of an organisation (ISO, 2009).

Risk analysis seeks to understand the risk source, cause, consequence, impact, likelihood and controls needed (ISO, 2009).

Risk evaluation is a process used to compare the risk analysis outcomes with established risk criteria, which is based on organisational objectives, to ascertain what action should be taken (ISO, 2009).

Risk treatment involves selecting and implementing decisions to address the risk. Risk treatment options include avoiding the risk, removing the risk, implementing measures to reduce either the likelihood or the consequence of the risk, sharing the risk or exploiting the risk to take advantage of an opportunity (ISO, 2009).

Monitoring focuses on having oversight of a process, to assess changes in performance , to ensure that issues are identified and improvements are made (ISO, 2009).

Reporting is part of risk governance and is a means of documenting and communicating risk management activities. Risk reporting can supplement decision making and provide a view of risk exposures (ISO, 2009).

2.2.4 Global technology, media and telecommunications industry key risks

The risk profile of the telecommunications industry has grown to include technology and media, as telecommunications companies have expanded their offerings to include music, video, gaming, streaming, cloud services and the internet of things (IoT) in addition to their traditional service offerings. The survey results shown in Figure 2.1 below identify the key industry risks across the technology, media and telecommunications industry for 2019 to 2021.

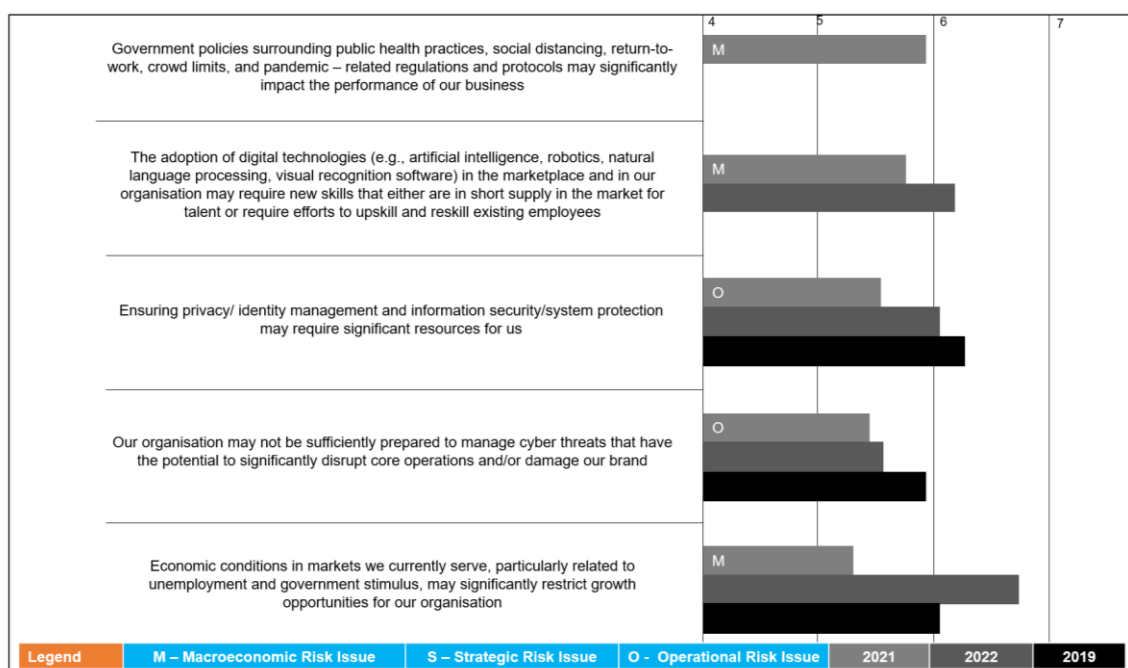


Figure 2.1 : Top risks for 2021 and 2030 – Technology, media and telecommunications industry perspectives (adapted from Protiviti, 2021)

The survey shown in Figure 2 was conducted by Protiviti, which is a global consulting company. The company's annual survey focused on the top risks for 2021 and 2030 from the technology, media and telecommunications industry perspectives (Protiviti, 2021).

The survey targeted 1081 participants from across the globe (Protiviti, 2021). Respondents indicated that more resources are required to be allocated to privacy and information technology (IT) security to better manage risk exposure (Protiviti, 2021). There was also a view that the impact of disruptive technologies has hampered the ability to businesses to manage risks (Protiviti, 2021).

In its Telecommunication Risk Factor Survey, professional services firm BDO focused on the future risks within the telecommunications industry. A future risk identified related to an organisation's inability to adopt new technologies internally (BDO, 2021). The survey noted that telecommunications companies introduce new innovative solutions to customers; however, the digitalisation of internal processes is not made a priority and there is a chance of the companies falling behind competitors that implement digital solutions to improve internal operations (BDO, 2021).

From assessing the Protiviti top risks survey together with the BDO survey, it is evident that the risk exposure is increasing, and organisations are unable to mitigate the risks adequately.

2.2.5 Relationship between Artificial Intelligence and risk management

Innovation and advancements in technology such as AI have pushed organisations to adopt AI technologies to improve operational efficiencies and become more competitive (Lee et al., 2020). In many business scenarios, core business functions have accelerated the adoption of AI technologies while support functions such as risk management have been slow to adopt AI.

Technology-enabled organisations are generating and collecting enormous amounts of data from operations, requiring the core business and support functions such as risk

management to analyse the data to drive data-based decision making. Research conducted by Biolcheva (2020) revealed that the use of AI can help the risk management process achieve synchronisation, better efficiency and the ability to process substantial amounts of data (Biolcheva, 2020). This would allow risk management insights to be forward looking, to predict future trends and patterns in real time while complementing decision making (Biolcheva, 2020). Real-time AI-based solutions have allowed cyber security to be managed more robustly and proactively, in this way minimising cyber threats (Anwar & Hassan, 2017).

According to Leo et al. (2019), machine learning, which is a subset of AI, has been identified as a key technology for transforming risk management. Machine learning has the ability to build more accurate models that can identify complex patterns within a sizable dataset (Leo et al., 2019). The models will have the capability to be predictable over time (Leo et al., 2019).

The rapid advancement of technology and its knock-on effect on organisations have meant that organisations are faced with ever-increasing operational risks. In the case of a bank moving to digital distribution channels, to sell credit products, for example, the velocity of risk exposure is increased, bringing about the need for proactive risk management. According to Aziz and Dowling (2018), to mitigate and manage credit card risk, AI has been integrated into the credit card fraud process to identify suspicious transactions by monitoring customer behaviour patterns. This puts the organisation in a position where it can proactively monitor transactions and build in alerts, based on the level of risk (Aziz & Dowling, 2018), and demonstrates how AI can add value to a process.

In relation to the ISO 31 000 risk management process, the Federation of European Risk Management Associations (FERMA) indicates that AI can be used to improve risk identification, analysis and assessment, monitoring, treatment and the risk process (FERMA, 2019).

AI has the ability to decrease risk management exposures by allowing a risk process to identify issues, assess the causes of these issues and respond at a faster pace (Dialogic Innovation, 2020).

The findings of the studies discussed above reveal that AI can positively contribute towards transforming risk management activities; however, the embedding of AI will

require building blocks to be in place. These include access to big data, machine learning models and computer processing power. Collectively, the building blocks can contribute to the integration of AI into a risk function.

From a South African perspective, limited research is available around the topic of AI and risk management. Research conducted by Jooman (2019) about the impact of AI on the future of internal audit revealed that the influence of AI on South African internal audit functions is in its infancy phase and there is a level of uncertainty regarding the implementation of AI within the internal audit function. This has meant that AI has not had a significant impact within the profession (Jooman, 2019). Since internal audit and risk management functions are assurance functions within the combined assurance model, the potential exists that risk functions in South Africa are faced with similar challenges.

In South Africa, the social challenge related to the high level of unemployment in the country may complicate decision making around the adoption of AI (BusinessTech, 2019). The implementation of technology may allow for efficiency and cost cutting while, on the other hand, the efficiency may result in unemployment (BusinessTech, 2019), which may contribute to the uncertainty around technology or AI adoption.

However, the benefits associated with AI adoption should not be ignored, according to Aziz and Dowling (2018). For example, when AI is integrated into credit risk processes, the ability to assess credit default is improved and reduces credit risk exposure as AI machine learning technologies outperform traditional approaches (Aziz & Dowling, 2018).

FERMA has also highlighted key benefits that risk management could take advantage of by implementing AI solutions. These benefits relate to the processing of large amounts of data, both unstructured and structured; efficiency improvements by optimising risk management processes; the ability to provide predictive and real-time oversight of exposures to improve response times; and the facilitation of improved decision making by having more visibility of and insight into risks (FERMA, 2019).

Although research has been conducted on the application of AI in risk management, there is still a gap and consequently an opportunity for further research to cater for AI application within a risk function in the telecommunications industry, as current

research focuses on specific risk types such as credit risk, market risk, fraud risk and financial risk (Leo et al., 2019).

2.3 Challenges associated with Artificial Intelligence implementations

AI presents several opportunities to improve organisational operations, advance the delivery of healthcare, improve education and overall allow society to innovate and increase productivity through AI democratisation (UP, 2018). However, there are challenges which could prolong and prevent the successful implementation of AI technologies.

These challenges stem, firstly, from the lack of availability of appropriate data, as data sources are held in silos across different business units, which hampers the ability of businesses to organise data in a manner that allows for AI technologies to process and learn from the data successfully (Aziz & Dowling, 2018). Data is a key input into the AI solutioning process; for an AI solution to be effective and deliver results, large amounts of data are required to teach and refine the solution (UP, 2018). In South Africa, legislation such as the Protection of Personal Information Act 4 of 2013 (POPIA, 2021) governs the processing of data, which creates a barrier to obtaining the large amounts of data needed.

The AI skills' gap is a second challenge that has hampered the further development and progress of AI adoption. There is a need for public and private institutes to reskill and equip employees with skills that are relevant for the 4IR (UP, 2018). Skill shortages can negatively impact growth in an economy, according to UP (2018), with skill shortages hampering growth in South Africa by 9% in 2017. To manage the issue, organisations have outsourced specialised technical development. According to Leo et al. (2019), the adoption of AI technologies has been hampered by the unavailability of suitable algorithms, which demonstrates the need for adequate skills to create these.

The third challenge concerns the adequacy of AI solutions. According to Aziz and Dowling (2018), there are issues around the accuracy of AI solutions. Solutions need to be adequately tested and evaluated on a regular basis to determine if they are working as intended and to manage exposures (Aziz & Dowling, 2018).

Ethical usage of AI and bias related to how AI solutions are coded make up a fifth challenge and one that has not been fully addressed. AI solutions may potentially be

hard coded with rules that discriminate against race, gender and sexuality (Aziz & Dowling, 2018). These will cause distrust of AI solutions and further draw back the adoption of AI.

2.4 Organising framework

An organising framework was drawn up for the study according to the concepts identified in the literature review as central to AI and risk management and the theoretical framework chosen as the theoretical foundation of the study. The organising framework includes the key concepts of the study together with the theoretical approach of the research and demonstrates the subsequent effects of AI technology on risk function towards achieving the objectives of the study. Figure 2.2 provides a structural view of the framework and demonstrates how AI, the sub objectives and overall objective links together.

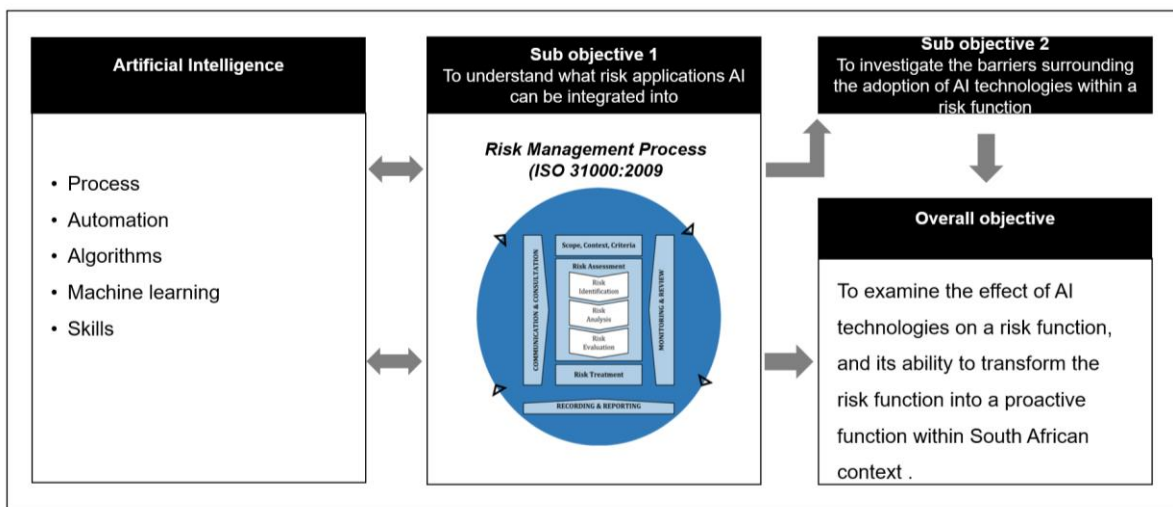


Figure 2.2: Organising framework

2.5 Conclusion of literature review

The literature review provided a basic understanding and view of the field of AI and the risk management process as outlined by the ISO, which provided a basis for understanding the overall workings of each concept. The review of relevant literature demonstrated the benefits of AI, such as the ability to gain operational efficiencies, create competitive advantages and digitalise manual processes generally. The risk

management analysis provided a view around the workings of the systemic risk management process together with current key industry risks, which potentially provides areas for AI implementation to mitigate the subsequent risks.

The relationship between AI and risk management was unpacked from previous studies to identify specific applications of AI in relation to risk management and identify gaps in the AI and risk management relationship. Key challenges include having access to big data, appropriate algorithms and processing power to implement AI solutions successfully.

The challenges related to AI implementations were examined and the following key challenges were demonstrated: skill shortages, availability of data, access to algorithms and ethical issues related to AI usage.

From the literature review, three propositions were drawn up.

Proposition 1

The increased adoption of digital technologies within the telecommunications industry in South Africa necessitates the integration of AI into the risk management function.

Proposition 2

AI adoption has the ability to accelerate risk management processes to proactively manage exposure.

Proposition 3

The implementation of AI solutions within a risk function requires an understanding of AI.

Chapter 3: Research Methodology

The following chapter presents an overview of the research methodology that was adopted to conduct the research study. Context around and details of the research approach, design, data-collection method and analysis, population and sampling, and ethical considerations are presented in the chapter.

3.1 Research approach

The study used an exploratory research approach to gain an understanding of the relationship of AI with a risk management function within the telecommunications industry. Owing to the limited research conducted on this topic within this specific industry, an exploratory approach was considered useful, as it allowed the researcher to collect data and test the applicability of AI adoption in a risk function within the telecommunications industry (cf. Creswell, 2014).

3.2 Research design

In its research design, the study adopted a qualitative approach. As part of this approach, face-to-face interviews were conducted, with structured and semi-structured questions. The approach allowed for the collection of new data to understand new perspectives brought to the study by the participants.

3.3 Data-collection methods

To obtain specific insights within the telecommunications industry, qualitative semi-structured interviews were conducted. The interviewees consisted of middle and senior managers who had agreed to participate in the study. The intention of interviewing this specified group was to understand the participants' views and opinions (Creswell , 2014) as they related to the research problem.

3.4 Population

The population consisted of participants who at the time of the study currently employed within the telecommunications industry from the risk management fraternity and individuals who had previously worked in a risk management function within a telecommunications company. Experienced risk management professionals were used as a basis for the extrapolation of the study.

3.5 Sampling

The study used a purposeful sampling approach, which allowed specific participants to be selected (Creswell , 2014). Participants were identified based on the level of risk management experience with a minimum of five years of working experience within the telecommunications risk management function. A total of 20 participants were interviewed from 4 telecommunication companies.

The 20-participants consisted of risk professional from the following risk management verticals.

- Compliance risk – 2 participants
- Enterprise risk – 4 participants
- Fraud risk – 3 participants
- IT risk – 3 participants
- Operational and strategic risk – 1 participant
- Regulatory risk – 1 participant
- Risk, compliance and regulatory – 5 participants
- Sustainability risk – 1 participant

Participants were encouraged to contribute ideas and opinions as the research sought to improve the risk management function, allowing participants to have an opportunity to shape future research on the topic.

3.6 The research instrument

An interview guide was used as the research instrument. Interview questions were captured in a schedule and followed a semi-structured format. The questions were derived from the study objectives and insights from the literature review. The interview guide is attached as Appendix C.

3.7 Procedure of data collection

Virtual one-on-one interviews were facilitated through online meetings with the identified participants. The interview guide was used to facilitate the interview. The interviews were recorded on Microsoft Teams and captured on a transcript.

3.8 Data analysis and interpretation

Interviews were conducted with experienced telecommunications risk professionals, who were expected to provide rich insights into the research problem. The interview recordings and transcripts were used to identify common themes. The data obtained was then used for thematic coding and evaluation by using Atlas Ti software, which assisted to analyse data, identify themes and patterns.

3.9 Limitations of the study

A limitation of the study was that participants might provide insights based on false pretences due to the negative perceptions related to technology replacing jobs.

3.10 Transferability, credibility, dependability and confirmability

Transferability, credibility, dependability and confirmability are important for ensuring trustworthiness in qualitative research.

3.10.1 Transferability

Since the study was specific to the telecommunications industry, transferability was not a priority. However, from a technology perspective, transferability is possible and

was achieved by thick description, which is a method in which a detailed account of data collection is maintained (Statistics Solutions, 2021).

3.10.2 Credibility

Participants that met specific criteria were chosen to be interviewed, to ensure that their inputs were relevant and credible. To ensure that the data collected was credible, i.e., that it accurately reflected what the participants had said, member checking was applied. This involved the researcher sharing interview data and conclusions with the participants for their comments and corrections (Statistics Solutions, 2021).

3.10.3 Dependability

Each process undertaken during the study was documented and reported on, to ensure that each step was evidenced and that the study could be replicated (Creswell, 2014). The supporting documentation was reviewed by an external reviewer for scrutinisation.

3.10.4 Confirmability

The data supporting the research findings was captured in an audit trail to ensure that the data-collection process, analysis of data, interpretations and themes were recorded and could be confirmed (Creswell, 2014).

3.11 Demographic profile of participants

A profile of the participants was drawn up according to their risk management experience within the telecommunications sector and the sample aimed to have a 50% gender split between female and male participants.

3.12 Ethical considerations

Participants were provided with an outline of the purpose of the study, including the scope, the intention of the study and an outline of why and how all information would be processed. Prior to each member of the sample participating, their consent was obtained. All data was kept confidential and anonymised for analysis and reporting. (See Appendix A for the participant information sheet.)

3.13 Summary

The chapter commences with an introduction, thereafter illustrates the research design, including the population, sample size, instrument utilised and ethical considerations. A qualitative research approach was adopted using a questionnaire to facilitate face-to-face interviews. Subsequently, the obtained data was gathered and analysed for presentation.

Chapter 4: Presentation of Findings

4.1 Introduction

The following chapter highlights key findings, themes and concepts from the study. A qualitative research approach was adopted and focused on interviewing risk management professionals who had experience within the telecommunications industry.

The presentation of findings has been structured into three sections to align them with the research propositions.

- Findings pertaining to Proposition 1: The increased adoption of digital technologies within the telecommunications industry in South Africa necessitates the integration of AI into the risk management function.
- Findings pertaining to Proposition 2: AI adoption has the ability to accelerate risk management processes to proactively manage exposure.
- Findings pertaining to Proposition 3: The implementation of AI solutions within a risk function requires an understanding of AI.

4.1.1 Participant profile –risk management role

The data-collection process involved the interviewing of 20 risk management professionals who performed different roles within a risk function. The points below provide a collective view of the number of organisations and participants who contributed towards the study.

- Company A – 1 participant
- Company B – 2 participants
- Company C – 5 participants
- Company D – 12 participants

The respective roles fulfilled by the participants within the risk management function and the number of participants that fulfilled each role are shown below.

- Compliance risk – 2 participants

- Enterprise risk – 4 participants
- Fraud risk – 3 participants
- IT risk – 3 participants
- Operational and strategic risk – 1 participant
- Regulatory risk – 1 participant
- Risk, compliance and regulatory – 5 participants
- Sustainability risk – 1 participant

4.1.2 Outcomes of thematic analysis

Table 1 provides a view of the codes and themes generated during the thematic analysis. The table highlights key themes which are linked to the research objectives.

Table 1: Codes and themes generated during the thematic analysis

Findings of thematic analysis codes	Themes	Research objectives
Proactive risk function Reactive risk function Hybrid risk function Risk technology adoption Insufficient risk support Risk support effectiveness Adequate risk support Sufficient risk support provided Aware of risk improvement projects Unaware if AI is being used for risk Unaware of risk improvement projects Effectiveness of AI on risk management AI benefits to risk management	Risk function is still predominately traditional in nature Risk support provided to business requires improvement AI has the ability to transform the risk management function	To examine the effect of AI technologies on a risk function, and its ability to transform the risk function into a proactive function within the South African telecommunications industry
Criteria to identify processes for AI integration Improved response times	Successful AI use cases within the risk function	To understand what risk applications AI can be integrated into

Findings of thematic analysis codes	Themes	Research objectives
No improvement on response times Risk process to be enabled with AI AI risk use case	Significant need for AI adoption within the risk function Opportunities for AI adoption	
Fair understanding of AI Familiar understanding of AI Good understanding of AI Limited understanding of AI AI challenges AI implementation challenge AI skills barrier Mitigating AI implementation challenges Risk by design	Understanding of AI is fair with room for improvement Risk management challenges related to AI adoption	To investigate the barriers surrounding the adoption of AI

4.2 Findings pertaining to Proposition 1: The increased adoption of digital technologies within the telecommunications industry in South Africa necessitates the integration of AI into the risk management function

To establish whether Proposition 1 could be confirmed, the study sought to understand the current nature of the risk function, in terms of the function's ability to provide business with adequate risk assurance; the risk function's ability to adopt technology at the same rate as business; AI initiatives and effectiveness of current AI initiatives; and the current nature of the risk function.

4.2.1 *The ability of risk function to provide business with adequate risk assurance*

Respondents were asked if the risk management function was able to provide sufficient risk support to business. The majority (50%) of the respondents indicated that the current risk function did not provide the necessary support to business, while eight (40%) respondents believed that their respective risk functions provided

adequate risk support to business. Two (10%) respondents did not comment. Figure 4.1 provides a view of risk management support towards support business.

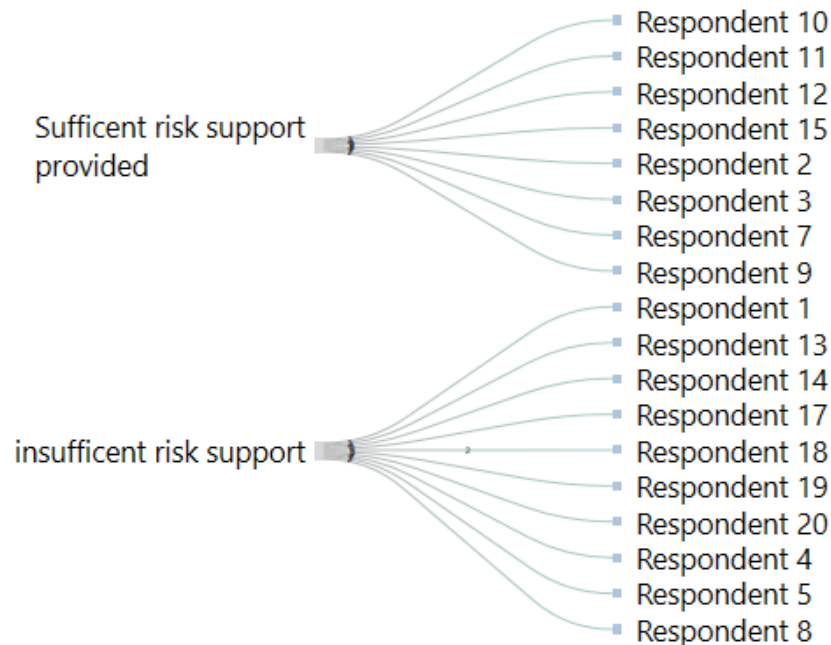


Figure 3.1: Risk management support provided to business

Forty per cent (40%) of the respondents indicated that their risk function provided sufficient support to business.

Respondent 10 was clear that the risk function was able to keep up with business demand.

“Yes, risk is able to keep up with business needs.” (Respondent 10)

Contributing factors that helped the risk function to provide adequate risk support and be proactive included the adoption of an agile approach to risk management and embedding of risk management processes within business. The following view was expressed by Respondent 9.

“Yes, we have adopted an agile approach to risk management, which has helped us to become proactive so that we respond adequately to any potential threats. If business is not aware of any emerging risk, we will bring this to the attention of business.” (Respondent 9)

Respondent 12 echoed the sentiments of Respondent 9 and highlighted that the risk function was able to provide sufficient support to business.

“Yes, risk can keep up with business to provide assurance. We have embedded risk assurance within business processes. We have adequate risk mitigating processes to provide comfort to business.” (Respondent 12)

Respondent 11 shared a similar view to Respondents 9 and 12 and referred to the process of integrating risk management processes into business processes as “risk by design”.

“Risk processes have been embedded into business processes to adequately provide risk support or assurance, we call this risk by design.” (Respondent 11)

The majority of respondents who indicated that the risk function provided insufficient support to business based their reasoning on various aspects.

Respondent 1 highlighted that the risk function was manual and traditional in nature, and there might be limited training initiatives to help the risk function to support business.

“I think that's a big gap in the risk environment because we are still traditional and very manual, and I don't even think there's a lot of training interventions that are preparing the risk functions to be able to operate in a way that will support businesses, with what business is currently doing with regards to artificial intelligence.” (Respondent 1)

Respondent 17 also highlighted that the risk function's traditional nature was restricting the function from providing appropriate assurance.

“No. The risk function as mentioned is very traditional and therefore they cannot keep up with business demands and provide proper risk assurance.” (Respondent 17)

Respondent 19 believed that the risk function was not versatile enough to support business.

“No, our traditional approach is not versatile enough to provide adequate risk coverage across business.” (Respondent 19)

Respondent 5 indicated that risk processes were unable to complement the agile nature of business.

“Currently no because of the nature of our environment as the telecommunications environment is very competitive and requires one to be extremely agile, to launch products in record times. With that being said, the current risks processes are not geared to complement the agile nature in general.” (Respondent 5)

It was identified by Respondent 8 that risk function could not keep up with business volumes in terms of providing risk support. For this reason, the function adopted a risk-based approach to focus on high-risk projects.

“Risk is unable to provide assurance across all projects or initiatives, this is due to the large number of business initiatives at play during the same time. A risk-based approach is adopted to focus on key projects.” (Respondent 8)

Respondent 20 highlighted that the risk function lagged behind business and echoed that the adoption of a risk-based approach was used to provide risk support that was focused on key areas.

“We do lag behind however, we provide risk assurance based on a risk-based approach and focus on key projects or initiatives but with that being said, AI would be beneficial for us and business to be able [to] expand our risk reach across a broader scope.” (Respondent 20)

Respondent 13 added that a risk function needed to have sufficient capacity to deal with business requests.

“Well, it all depends if your risk function is big enough to handle the business demand. I know with business they have new ideas every day and want to push on as soon as possible. We are not able to assess the risks and give the full attention to this.” (Respondent 13)

4.2.2 Risk function’s ability to adopt technology at the same rate as business

The interviews explored whether risk functions were on par with business in terms of technology adoption and implementation to enhance the risk function. In providing their views on this topic, 95% of the respondents agreed that the risk function was unable to keep up with business. The respondents’ rationales were based on various factors.

Respondent 8 attributed the risk function's inability to adopt technology to business receiving priority in preference to the risk function.

"No, we cannot keep up with business due to priority given to business as business makes money and risk plays more of a guarding role. There is room for risk to improve to increase technology adoption within risk." (Respondent 8)

Respondent 16 concurred that prioritisation was an issue, as risk management was deprioritised in comparison to business.

"To implement processes I would say yes, but to implement systems I would say no. That is where business gets more value as they bring in the money. You are a support function and may be given a small chunk of the budget and less priority. It is still a very manual approach." (Respondent 16)

Respondent 7 highlighted that the risk function's slow adoption of technology was related to the function being traditional.

"No, it is not fast paced, it lags. Risk is very traditional on how it works and still documents in Excel etc. These haven't changed. We are seeing tools been used but it only digitizes the spreadsheet, so still someone still has to input the data. It is subject to a lot of human intervention and evaluation. Nothing has changed except for the interface." (Respondent 7)

Respondent 19 shared a similar view to Respondent 7, arguing that the traditional nature of risk management negatively impacted the function's ability to adopt technology at the same speed as business.

"No, risk management is very traditional in nature and does not implement new systems in a hurry." (Respondent 19)

Respondent 17 went on to suggest that the traditional approach of the risk function had resulted in the slow adoption of technology, leading to the risk function being unable to meet business needs.

"No. Business always moves quick and develop new technologies, however the risk function is still very traditional and slow when it comes to developing new technologies. Very often the risk function cannot keep up with business demands." (Respondent 17)

Respondent 18 revealed that when it came to technology adoption, the risk function lagged behind business and, to address the gap, risk processes were included in business procedures.

“No, we have generally lagged behind business from a technology adoption perspective. To address this gap, we began embedding risk and controls into business processes.” (Respondent 18)

Respondents highlighted the following factors as contributing towards risk management being unable to adopt technology at a fast pace as compared to business. Findings included budget restrictions, risk management seen as a support rather than a revenue-generator function and risk technology being in its infancy stages of technology development. Key quotations related to the contributing factors are provided.

Budget constraints were highlighted as a factor that impeded the ability of the risk function to adopt technology. This view was expressed by Respondent 11.

“No, we don’t adopt technology as a fast pace due to budget constraints.” (Respondent 11)

Respondent 10 noted that although the risk function could adopt technologies, restrictions were caused by budget constraints.

“Risk management are able to adopt new technologies however, budget constrains restricts the function.” (Respondent 10)

Respondent 5 highlighted that risk technology is in its infancy stage of development and this contributes towards the risk function being unable to adopt technology to improve risk processes.

“Yes and no because from a risk management technology perspective, risk is still in its infancy stages whereas risk management as a key capability is well into its a mature stage.” (Respondent 5)

Respondent 10 noted that the availability of risk management solutions within the market is limited, which corroborates Respondent 5’s statement.

“There are limited risk system options available for procurement.” (Respondent 10)

Respondent 20 re-emphasised the point about the limited number of risk solutions available and further indicated that these solutions are not fit for purpose.

“I don’t think you can compare us to business. In risk management we have not had a revolutionary system launched in the risk world, we do have off the shelf risk systems, but these are not the most friendly. What is in the market, is not agile because it may have been designed [by] old school risk managers. Yes, we do develop in house risk systems but it’s slow.” (Respondent 20)

4.2.3 Artificial Intelligence initiatives used and their effectiveness

During the data-gathering process, respondents were asked whether their risk functions currently made use of AI technology. Six respondents indicated that they were unaware that AI was being used in their risk functions.

Figure 5 provides a view of these respondents. Key quotations of their opinions follow the figure.

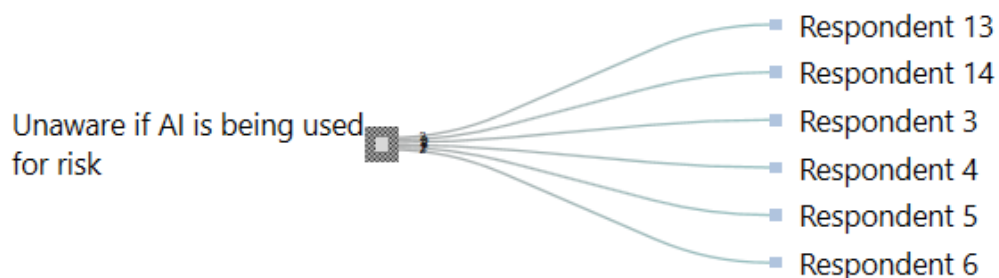


Figure 4.2: Awareness of whether AI is being used within the risk function

Respondent 5 was unaware of current AI solutions being utilised by the risk function and believed that this was unlikely.

“Currently, I am not aware of AI systems within the risk function, its more process automation rather than intelligence.” (Respondent 5)

The same view was expressed by Respondent 4: *“At the moment, I would say No”* (Respondent 4), and Respondent 14: *“Within the risk function no, we have not implemented any AI technologies”* (Respondent 14).

The interviews also sought to understand the effectiveness of current AI initiatives where they were incorporated into a risk function.

Respondent 2 indicated that AI had helped the function to identify risks at a faster pace with minimal manual intervention.

“AI has helped to identify risk quicker as opposed to human task or intervention.”
(Respondent 2)

Respondent 7 supported the view of Respondent 2.

“It is improved the ability to identify risks instead of relying on manual identification. We now have maximum coverage for this area.” (Respondent 7)

Respondent 9 highlighted that AI had created efficiencies within the risk management function.

“It has had a positive effect in that it will drive efficiencies, proactive risk management and flexibility.” (Respondent 9)

Respondent 11 indicated that AI had assisted to decrease their organisational risk by realising savings and improving the image of risk management.

“AI has helped to reduce organisational risk. A good example is fraud risk and savings gained from preventing fraud which improves our reputation and enhances confidence in risk management.” (Respondent 11)

Respondent 18 added that improved risk management with the use of AI had added value to the customer and enhanced the organisation’s brand.

“AI has helped to improve our risk management, improve customer experience and helped the organisation to build trust.” (Respondent 18)

Respondent 16 shared similar viewpoints to that of Respondent 18.

“This brings ease to an employee because they not working hard but working smart in finding out what is going to happen before the time. This offers client satisfaction and improves the organisation’s reputation.” (Respondent 16)

Respondent 12 added a new dimension of AI within risk management, whereby AI had assisted to expand the function’s capability in real time.

“It has brought about the capability to assess risk at the edge. This refers to when we interact with a customer via our channels, we are able to assess risk in real time as our channels are linked to our central AI engines.” (Respondent 12)

Respondent 15 demonstrated that current AI initiatives within the risk function had improved the risk management function.

“Yes, natural language processing and advance voice biometrics, facial recognition, using AI to predict issues on the network. Use of AI to prevent SIM swap and subscription fraud. These are some of the basic technologies we have implemented.” (Respondent 15)

Respondent 3 highlighted a contradictory view as compared to the respondents above. This respondent indicated that the full value of AI deployed within the risk function had not been fully understood.

“To date, minimal AI implementations have been undertaken into the regulatory space. The complete value of AI has not been realised.” (Respondent 3)

4.2.4 Current nature of the risk function

To understand the nature of the risk function in terms of the function’s proactiveness and reactiveness, as these characteristics are vital when managing risk, respondents were asked to share their views. Fifty per cent of the respondents indicated that their current risk management function was reactive by nature, 45% of the respondents described their risk functions as a hybrid of proactiveness and reactiveness while 5% believed that their risk function was proactive in nature. Figure 4.3 provides insight into the nature of the risk management function.

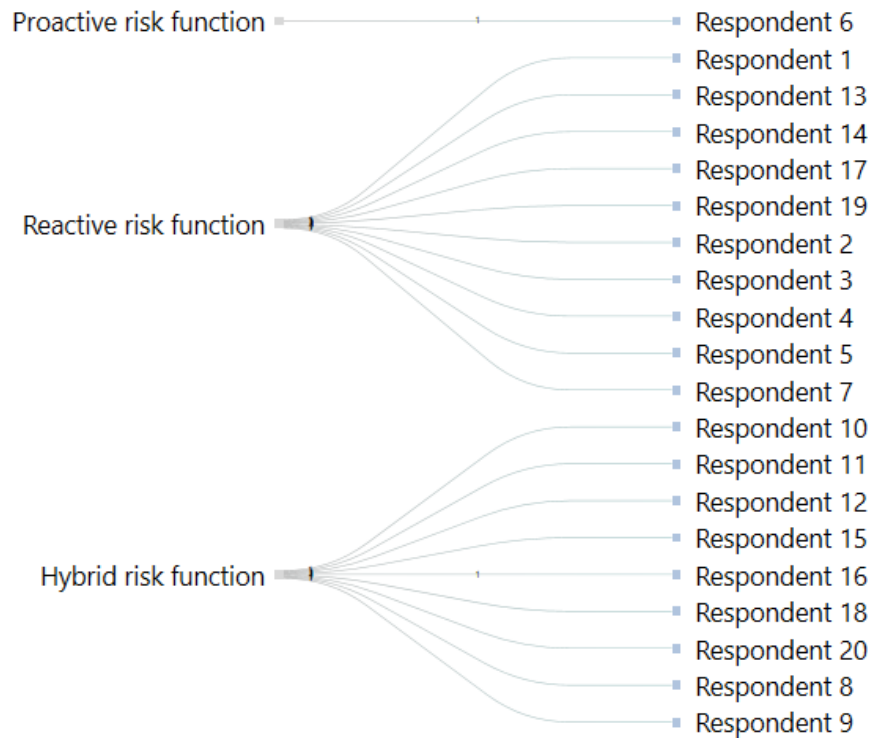


Figure 4.3 : Nature of risk management function

Respondents who leaned towards the risk function being reactive in nature highlighted several contributing influences.

Respondent 1 indicated that current risk function processes were manual, which resulted in the risk function being reactive.

“Very reactive. In our environment the current process is very manual and reactive.”
(Respondent 1)

This view was also expressed by Respondent 5, who also alluded to limited proactiveness and automation within the risk function.

“Reactive as the risk function has too many people involved, too many processes, too little automation and proactiveness involved.” (Respondent 5)

Respondent 14 highlighted that inefficiencies related to risk management processes contributed towards the reactiveness of the risk function.

“We are proactive in that we make sure we try to implement some kind of risk management processes but the efficiencies of the process itself and what it needs to accomplish, I would say we are very reactive. We are reactive because things almost

happen to us and then we think about what we should put in place. COVID is an example, we should have had something in the BCP [Business Continuity Plan] plan some controls with the understanding we are humans and that there could be some sort of sickness or virus could happen.” (Respondent 14)

Respondent 19 added that limited financial and human resources restricted the risk function from being proactive.

“Very reactive due to the limited human and financial resources available.” (Respondent 19)

The 45% of respondents who leaned more towards their risk functions adopting a hybrid risk management approach expressed the following views.

Respondent 8 indicated that their risk function was 80% reactive and 20% proactive and highlighted the integration of AI within the fraud risk management process.

“At the moment it’s hybrid, both proactive and reactive. Proactive in the sense that we have used AI to do deep analysis to assess fraud. However, there are some false positives. We are about 20% proactive and 80% reactive.” (Respondent 8)

Respondent 11 was aligned to the view of a hybrid risk management being adopted and further indicated that this depended on the type of risk streams as some risk streams might be more proactive than other streams.

“The function is a bit of both, that is proactive and reactive in nature and it also depends on the risk stream. Areas such as cyber and fraud risk are very proactive while enterprise risk is more reactive. The stream may dictate the nature of risk management.” (Respondent 11)

Although Respondent 12 alluded to the risk management function as adopting a reactive and proactive approach, this respondent also stressed the need to become more proactive with the use of AI.

“From a fraud and enterprise risk perspective we have risk processes built into business process to identify risks ahead of time, an example is before a product is launched risks are identified and business would need to address the potential issues. We are proactive to some extent but generally more reactive. AI can help us to become more proactive.” (Respondent 12)

Respondent 16 was of the view that the risk fraternity was at the beginning of a technological revolution.

“Certain parts are proactive and some reactive. Industries are still getting use to technology in risk management and we still building. If I have to give a percentage, it would 70% very reactive.” (Respondent 16)

4.3 Findings pertaining to Proposition 2: AI adoption has the ability to accelerate risk management processes to proactively manage exposure

To understand whether current AI initiatives within the risk function have improved risk response times to better manage risk exposure, this topic was explored with the respondents. This exploration included the criteria one should use to identify risk management processes that would be appropriate for AI adoption and which processes could be enabled with AI. Respondents were asked to suggest use cases that they thought would be ideal for integrating AI to better manage risk exposure. Respondents were also asked to share their experience regarding whether AI could accelerate a risk function by managing risk more proactively.

4.3.1 The ability of Artificial Intelligence initiatives to improve risk response times for better risk exposure management

Respondents indicated that overall response times were improved and enabled the function to be better positioned to respond to risks and manage risk exposure. Although AI had provided benefits to the risk function, respondents also noted that there was a need to improve response times.

Respondent 1 highlighted that AI integrated into fraud risk management improved response times.

“Yes, AI has improved our risk response times from a fraud perspective.” (Respondent 1)

Respondent 7 indicated that AI increased response times by allowing for real-time responses.

“Yes, it has. This is purely because the process was automated and integrated with intelligence. It is real time and there is no paperwork from one team to another. It will alert what are the risks.” (Respondent 7)

Respondent 11 confirmed that AI had assisted the function to manage risk exposures with enhanced response times: *“AI has allowed us to better identify and respond to risk and indirectly improving response times”* (Respondent 11). Respondent 18 echoed a similar perspective: *“Turnaround times have drastically improved and limited our risk exposure”* (Respondent 18).

Respondent 12 demonstrated that AI had enabled the function to facilitate risk decisions at the edge at a faster pace.

“Yes, response times are much quicker as we can make risk decisions at the edge.” (Respondent 12)

Respondent 8 indicated that AI had helped the risk function’s response times to some extent but suggested that there were opportunities for further improvement.

“AI has assisted us in certain aspects, but response times have not improved much as there are still several false positives, which takes times to unpack, therefore delaying our responses.” (Respondent 8)

Respondent 9 felt that AI helped with real-time information and engagement but noted that response times still needed improvement.

“Yes, it did, real-time engagement with business with real-time information improved our response times. However, we can still improve.” (Respondent 9)

Respondent 20 also alluded to the need for further improvement of response times.

“It has improved but there is still room improvement.” (Respondent 20)

4.3.2 Criteria for identifying appropriate risk management processes for Artificial Intelligence adoption

Prior to AI being integrated into a process, it is important to understand what criteria one should use to identify the appropriate risk management processes for AI adoption. Respondents highlighted the key criteria as set out in Figure 7.

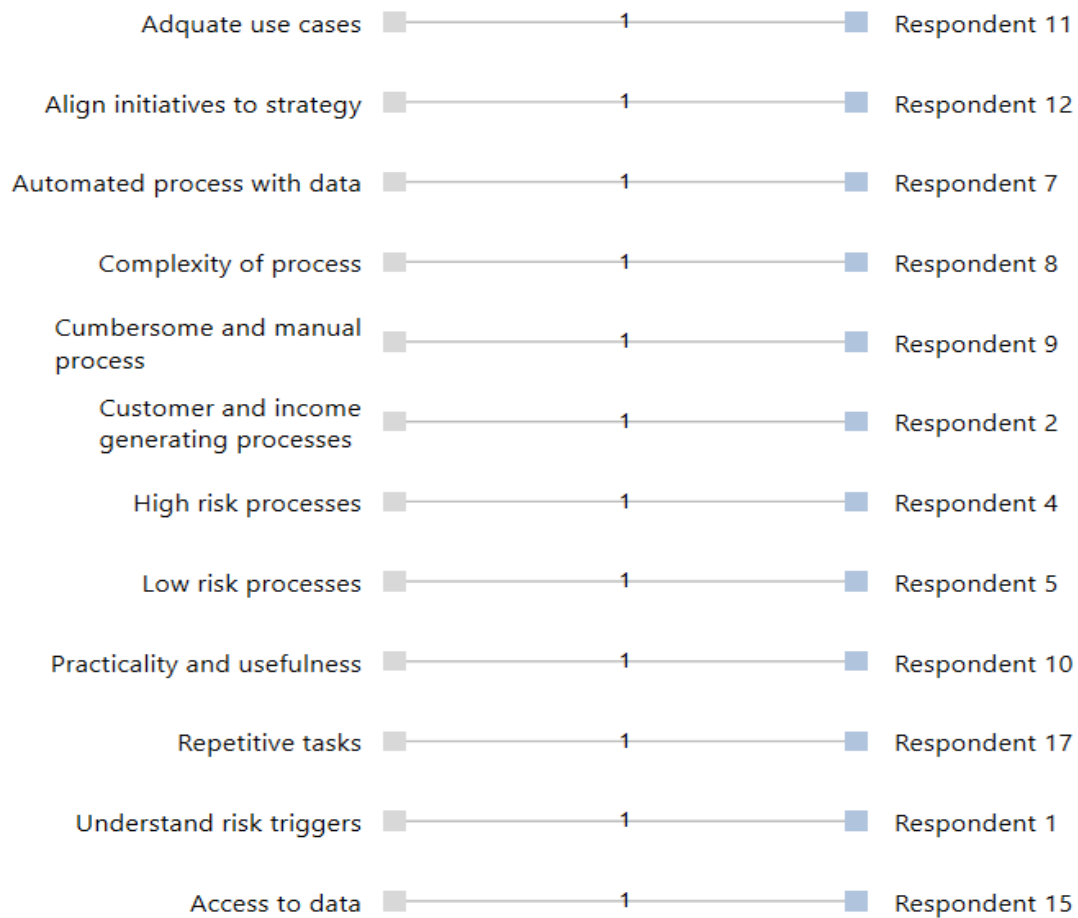


Figure 4.4: Criteria to identify risk processes for AI integration

Respondent 1 highlighted the need to understand risk triggers.

“I think once the environment understands its risk triggers those can be configured into a program.” (Respondent 1)

Respondent 2 suggested that attention should be given to income-generating and customer processes.

“Focus on processes, tools, technology, and system applications that are more customer focus, income generating etc.” (Respondent 2)

Respondent 4 proposed the need to consider high-risk and core processes.

“I would rather look at your high-risk processes from a revenue point of view to say if this process were to be impacted from a revenue point of view, how much will be impacted. I will also look at the core processes in the business.” (Respondent 4)

Respondent 5 recommended focusing on low-risk processes as key criteria. In the event of an AI initiative failing, the impact would then be low.

“Obviously, you have to start from the low-risk processes because you don't want to start with medium or high-risk processes, to target low hanging fruit and process which will not expose us too much, if AI does not work.” (Respondent 5)

Respondent 11 proposed that use cases needed to be adequate, with no dependency on human interference.

“Ideally use cases which does not require human intervention to evaluate the outcomes.” (Respondent 11)

According to Respondent 12, ideally initiatives should be aligned to business strategy with a good understanding of the risk appetite, to determine the type of controls required.

“We should look at the business strategy and align our initiatives to the strategy. Understand risk appetite to determine how that risk should be managed as this will dictate if proactive or reactive controls can be used to manage the risk. Understand technology visions which will help to drive process transformations.” (Respondent 12)

Respondent 15 highlighted the need for structured and quantifiable data to be available as a key criterion.

“We must have data and be able to structure the data. We must have quantifiable data with appetites or tolerances established.” (Respondent 15)

Respondent 17 advised that repetitive and low value tasks should be considered.

“I would look at the process risk ratings, low value tasks which are repetitive.” (Respondent 17)

Respondent 19 agreed with Respondent 17 and suggested that manual processes should also be considered.

“Manual or repetitive risk processes should be embedded with AI technology.” (Respondent 19)

Respondent 18 indicated a need to remove subjectivity, with processes that contained subjectivity considered for AI integration.

“I would look at the high-risk business processes across, such as financial and regulatory processes. Understand the risk exposure of these processes, have the processes been automated or leaning more towards being manual, as this will provide an indication if there is room to implement AI. If processes are subjective, we should try to introduce some element of AI to remove the subjectivity.” (Respondent 18)

4.3.3 Risk management processes enabled with Artificial Intelligence that would ensure relevant risk management

To ensure that the integration of AI into risk management is relevant and addresses a need, respondents were asked which risk management processes could be enabled with AI.

Respondents highlighted the risk identification, assessment, monitoring and reporting processes as key processes for AI adoption.

Respondent 1 suggested that the risk identification and assessment processes could be integrated with AI.

“I think risk assessment, the identification and rating processes can be configured with AI.” (Respondent 1)

Respondent 2 agreed with Respondent 1’s opinion and added that the risk reporting and monitoring processes should be considered as well.

“Risk identification, assessment, monitoring and reporting.” (Respondent 2)

Respondent 8 concurred with the view of Respondent 2 in terms of risk processes related to the risk identification and monitoring processes, for the enablement of AI.

“I think identification and monitoring can be integrated with A.” (Respondent 8)

Respondent 4 indicated that the analysis and evaluation processes could be enabled with AI.

“I would say risk analysis and risk evaluations. If you look at the application and where you would analyze, I believe these processes can be easily automated. These are the key processes to automate and if it can be done then you will be able to manage or control your risks adequately.” (Respondent 4)

Respondent 11 provided insights as to how AI could be used to perform risk identification through horizon scanning and monitoring through using AI to monitor key risk indicators. Respondent 11 noted that risk evaluation can be enabled with AI.

“Risk identification, where algorithms can be used for horizon scanning to identify potential risks. Monitoring and reviewing processes, for example where key risk indicators can be monitored and if there are breaches, an alert will be reported or flagged. Risk evaluate, AI can be used to evaluate simple risk measures.”
(Respondent 11)

Respondent 16 suggested that the risk assessment process could be enhanced with AI, indicating that integrating AI within risk assessment would provide the function with a complete view of risk.

“I think risk assessments can be enabled with AI. You have a thousand risk assessments, now all risk assessments should be available in a system that everyone in your risk community has access to, but it is summarised based on the risks or project. Risk is sometimes not associated with fraud but with AI, it will give us a holistic view.” (Respondent 16)

Respondents 10, 12, 13 and 18 shared a different view from the majority of the respondents. These respondents believed that the end-to-end risk management process should be enabled with AI. The quotations below support their viewpoints.

Respondent 10 believed that the end-to-end risk management process should be enabled with AI.

“The end-to-end risk process which is dependent on the current process and level of automation.” (Respondent 10)

Respondent 12 underlined the traditional approach to risk management and highlighted that AI could transform the overall risk process.

“The traditional way involved people inputting data into applications. As far as those processes are concerned, AI can be used to transform the end-to-end processes, from risk identification through to reporting.” (Respondent 12)

Respondent 13 concurred with the views expressed by Respondent 10 and Respondent 12 and stressed the need to integrate AI within the life cycle of risk management and not just specific risk management processes.

“I would say the risk assessment process, actually the whole risk management life cycle can be enabled with AI.” (Respondent 13)

4.3.4 Ideal use cases where Artificial Intelligence could be integrated for better risk exposure management

It was important to understand from the respondents which use cases they considered ideal for AI integration to better manage risk exposure.

The respondents provided the following use cases: cases related to customer onboarding and financial processes; robots to answer frequently asked questions; cyber, fraud, privacy and compliance; and use cases involving the integration of systems.

Respondent 2 highlighted the need to embed AI into use cases related to customer onboarding, financial and third-party risk processes.

“Customer onboarding processes, financial processes and third-party risk management.” (Respondent 2)

Respondent 11 stressed the need to consider customer facing use cases as there was an opportunity to better manage risk, and to limit customer impact.

“Applications which are customer facing or applications that indirectly impact customers to better manage fraud and cyber risk.” (Respondent 11)

Respondent 20 further supported the use of financial use cases because such processes were mature in nature and understood.

“Financial and operational applications can be enabled with risk AI as these are mature, structured and well understood to applications and processes.” (Respondent 20)

Respondent 3 suggested a use case that involved the use of a robot to answer frequently asked questions.

“Maybe have AI and I am using these words loosely, have a bot where you literally allow the BOT to answer repetitive or common risk questions, the Bot could literally cover 20% of my workload and I can concentrate [on] other things.” (Respondent 3)

Respondent 12 recommend use cases associated with cyber, fraud and product reviews to be enabled with AI.

“Implementation of AI into fraud, cyber and product assessment applications. AI needs to cut across these applications to offer richer insights to manage risk.” (Respondent 12)

Respondent 16 supported the use of AI in use cases linked to cyber security and fraud risk management, highlighting the need to enhance the processes.

“I would say the management of cyber security, access management and enhancement of fraud monitoring.” (Respondent 16)

Respondent 9 indicated that owing to the regulatory environment in which their organisation operated, it was necessary to enable compliance use cases with AI.

“I think first we should look at compliance as we operate in a highly regulated environment. Identify which are high risk policies and regulatory requirements. Next would-be fraud risk, such as SIM swap fraud and stealing of personal data. These are two key processes before we move to enterprise risk.” (Respondent 9)

Respondent 17 further highlighted a compliance use case related to privacy compliance.

“I think that would be operational, privacy and cyber risk.” (Respondent 17)

Respondent 5 highlighted use cases that involved the integration of systems, which would allow the risk function to have additional data points to better identify potential risks.

“System X can be enabled with AI to become more intelligent. We also have various systems within the telecommunications industry, many of the systems operate in silos, if we can integrate these systems and enable them with AI, we will be able to have more data points to identify risks.” (Respondent 5)

Respondent 8 also stressed the need to have more access to data for monitoring in real time.

“AI should be embedded at a CRM [Customer Relationship Management] and network level, to have access to more data for real time monitoring.” (Respondent 8)

During the data-gathering process, some of respondents provided use cases related to new business streams being launched and developed by telecommunications companies.

Respondent 4 suggested that to manage risk related to the collections of insurance premiums, billing and subscriptions, the use cases should be integrated with AI.

“From a business point of view, the customer collections for subscriptions, whereas in insurance it would be collection of premiums. We must ensure that these processes are made real time. I would say billing and subscriptions as a business process should be enabled with AI to manage risk.” (Respondent 4)

Respondent 18 recommended that the payments’ process be integrated with AI to monitor payment transactions in real time.

“The payments process requires the movement of money, ideally we would want minimal human intervention to avoid human errors, therefore this process should be enabled with AI to assess abnormal transactions and flag issues in real-time.” (Respondent 18)

Respondent 18 went on to elaborate on how traditional telecommunications companies (Telcos) were evolving into technology companies (Techcos), and the need to have a holistic view of a customer’s risk profile across old and new business, to improve the management of risk exposures.

“Since there is no single view of a customer across traditional Telco products and new Techco products, there is a need have an overall view of the customer’s risk profile to better manage risk exposure. As the traditional Telco transitions into becoming a Techco by introducing new products and services like financial services, IoT (internal of things) and content services which are driven digitally, we need to adjust the lens we currently use to assess risk and embrace new technologies to transform our risk function to be able, to better manage risk.” (Respondent 18)

Respondent 15 stressed the importance of including a use case linked to content subscription, to manage fraud risk.

“A key use case lies within the content subscription fraud application as we can’t get authentication right.” (Respondent 15)

4.3.5 Respondent experiences regarding the impact of Artificial Intelligence on the risk function

To understand if AI can accelerate a risk function by enabling it to manage risk more proactively, respondents were asked to share their experiences in this regard. Respondents overall had a positive view of the impact that AI would make within a risk function and expressed a need for the risk function to integrate AI within the risk fraternity, to better manage risk exposures.

Respondent 1 indicated that AI had the capability to transform the risk function to improve effectiveness and proactiveness.

“As mentioned, AI has the ability to make the function more effective and proactive and assist risk to add business value.” (Respondent 1)

Respondent 11 suggested that AI would assist the risk function to foresee risks, to prompt responses that would lead to the proactive management of risks.

“AI will allow us to be able to predict potential risk scenarios ahead of time for us to adequately be prepared to respond to the risk. This will allow us to be more proactive.” (Respondent 11)

Respondent 9 added that AI would offer more insights regarding risk management.

“AI will allow risk management to be more proactive and offer more risk insights to business.” (Respondent 9)

Respondent 2 indicated that a risk process embedded with AI could be run continuously, to improve risk management processes.

“Risk will be more proactive than reactive. Now risk is currently reactive. With AI tools, processes can run for twenty-four hours and can improve risk management. The tool

on its own eliminates mistakes and may take shorter time to complete an assessment. Brings more accuracy as another benefit.” (Respondent 2)

Respondent 5 demonstrated that the use of AI would improve the function’s output to add business value.

“The use [of] AI will increase the output of the risk management function to be proactive in nature, improve response times and add more value to business.” (Respondent 5)

Respondent 8 indicated that AI would improve the risk function by allowing human resources to focus on complex risk tasks while AI managed the tedious facets of risk management.

“Definitely yes, if given time for AI and the machines to learn, it will allow us to more proactively manage risk. AI can be designed to focus on the mundane aspects of risks while people focus on the complex nature of risk.” (Respondent 8)

Respondent 15 provided the view that current risk management assessments were hindered by the reliance on humans to perform risk tasks. Respondent 15 alluded to AI assisting the risk function to process risks at a fast pace while increasing its risk-coverage scope.

“Yes, in general most risk assessments are delayed by a human’s inability to quickly analyse and provide a response. AI will be able to process risk scenarios at a much faster pace and be able to expand our risk scope as the tool will be able cover more.” (Respondent 15)

Respondent 18 stressed the need to move away from the traditional risk management approach and from depending on human abilities within the risk function.

“As Telcos are moving towards becoming a Techco and more digitalised, there is a need to embed AI into our traditional process and move away [from] human dependencies, to become more proactive in supporting business.” (Respondent 18)

However, Respondent 7 noted that although AI would assist to improve the risk function, there would be a need for human intervention.

“Yes, but human intervention will always be required to input those rules.” (Respondent 7)

Respondent 20 further added that risk management would always have a component of reactivity as, while AI could add a proactive benefit to specific risk areas, human involvement would still be needed.

“So, in certain areas AI can bring about proactiveness but there will be an element of reactivity as we still need human intervention in some instances.” (Respondent 20)

Respondent 12 believed that AI would assist a risk function to become more proactive; however, the risk function depended on organisational culture, which would determine how far it embraced technology.

“Proactive yes, but this is always hinged on the culture on the organisation. If the culture of the organisation is meant to be digitally minded, it is up to leadership to take the leap, to know which technologies are best suited and when.” (Respondent 12)

Respondent 10 shared a view that contradicted those expressed by the above respondents. Respondent 10 indicated that AI had brought about benefits to business and customers; however, whether it would benefit risk management enough to encourage investment in AI within the risk function was unclear.

“From a business perspective we have seen benefits which have assisted to reduce data capturing times, improved online customer experience allowing us to add more value to the customer. However, that’s also my question, what benefit will AI bring to risk management to warrant investment?” (Respondent 10)

4.4 Findings pertaining to Proposition 3: The implementation of AI solutions within a risk function requires an understanding of AI

To explore the level of understanding of AI among risk professionals, respondents were asked to indicate and elaborate on their level of understanding of AI, machine learning and automation. Respondents were also asked to describe the challenges they faced when implementing AI solutions and to suggest ways of mitigating these issues. The highlighted challenges assessed against the challenges highlighted in the literature review provides a view of the level of understanding of AI.

4.4.1 Level of understanding of Artificial Intelligence

Twenty-five per cent of the respondents indicated that they had a good understanding of AI, as a result of their current experience and involvement in related technology projects within the risk function. Figure 4.5 provides a view of respondents who indicated that their understanding of AI is good.

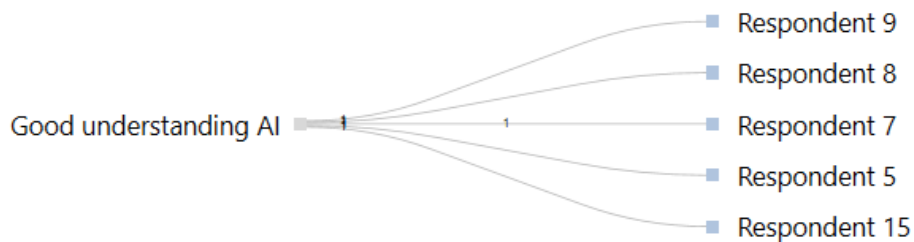


Figure 4.5 : Understanding of AI – good

Respondent 5 indicated that they had conducted research into AI, which had given them an understanding of AI.

“Yes, so funny enough AI and machine learning has sparked my interest and I have done some research into these concepts. AI is an algorithm that makes a decision based on information that has been inputted into it. Whereas machine learning uses game theory to do something in a specific way.” (Respondent 5)

Respondent 8 demonstrated a good understanding of AI owing to their experience with current transformational projects.

“I am familiar with the concepts, we have implemented a machine learning risk identification tool on the subscriber side of the business. I am aware of AI, optical character recognition, machine learning, robotics process automation, and neural networks.” (Respondent 8)

Respondent 9 highlighted that exposure to AI had helped them to gain a good understanding of AI.

“Yes, I am very familiar with the concepts. Risk has been pursuing AI and robotics. How can we use AI to enhance risk management so that risk is not a tick box exercise, improve proactiveness and enhances collaboration between other assurance

providers. So, the exposure to AI from where I am sitting has been awesome.”
(Respondent 9)

Figure 4.6 depicts the majority of 60% of respondents who indicated that they were familiar with the terminology.

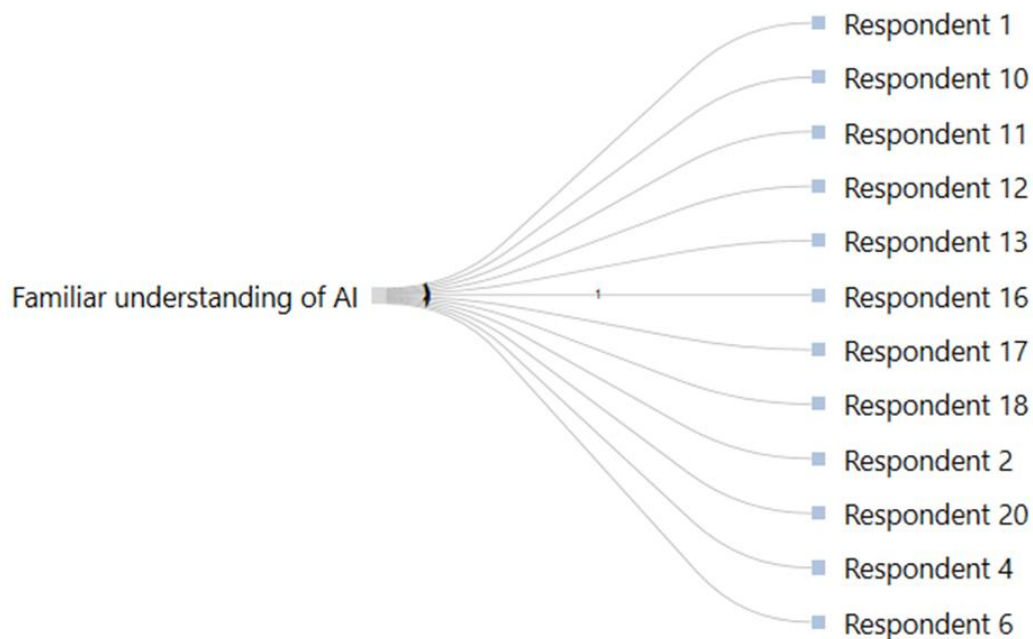


Figure 4.6 : Understanding of AI – familiar

Respondent 4 and Respondent 1 highlighted that they had some understanding of AI.

“Yes, I am familiar.” (Respondent 4)

However, they felt that there was room for improving their understanding of AI concepts.

“To some extent yes.” (Respondent 1)

However, from an observation perspective, only Respondent 2, who said: *“Yes, I am familiar with the concepts. My previous role we had a lot of automated tools and AI. Had a lot of sand boxing experiencing using these tools”* (Respondent 2), and Respondent 17, who said: *“Yes, I am familiar and have an understanding of what AI, automation and machine learning can do”* (Respondent 17), attempted to elaborate further.

Figure 4.7 demonstrates the number of respondents who have a limited understanding of AI.

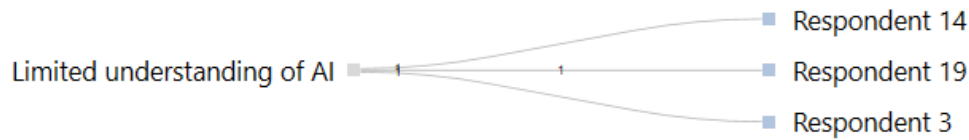


Figure 4.7 : Understanding of AI – limited

During the data-gathering process, three (15%) respondents highlighted that their understanding of the technology concepts in question was limited, with Respondent 14 answering as follows:

“I have limited understanding of the concepts.” (Respondent 14)

Respondent 19 indicated that this was due to their regulatory risk focus.

“I am aware of the concepts but I don’t have an understanding of the technology terms, due to my focus on regulatory risk.” (Respondent 19)

4.4.2 Challenges in implementing Artificial Intelligence solutions and ways of mitigating these challenges

To further unpack the understanding of AI implementation, respondents were asked to describe challenges faced when implementing AI solutions and how to mitigate these challenges. Key challenges identified included lack of skills, lack of reliable data, lack of stakeholder buy-in, poor organisational culture, budget constraints, limited business capabilities, business priority over the risk management function and regulatory challenges related to privacy.

Respondent 4 highlighted challenges related to budget constraints and the lack of will power to embark on AI transformations.

“I think one of the reasons why, is maybe the hesitance or lack of licensing to do so. There are also budget constraints where business will tend to prioritize the money-

making projects that will make revenue. It will be nice for us to be proactive, but it is a still [a] challenge.” (Respondent 4)

Budget constraints were echoed by Respondent 9: *“You might not have adequate budget requirements. Money might not be sufficient to cater for the deployment as well as the design and the configuration”* (Respondent 9), and Respondent 10: *“Risk management are able to adopt new technologies however, budget constrains restricts the function”* (Respondent 10).

Respondent 4, aside from noting budget constraints as a key challenge, highlighted privacy laws as a barrier, as these laws could potentially restrict data processing.

“I would say budget constraints, but also on the legal side. I will say the privacy laws could be one of the hindrances. To elaborate on this. It is largely due to the requirements of over processing.” (Respondent 4)

Respondent 8 acknowledged that since business needs are prioritised over the risk function, obtaining resources to drive risk initiatives was challenging.

“Obtaining internal resources is challenging as business needs are priority. Our system landscape is very complex.” (Respondent 8)

Respondent 8 indicated that to mitigate budget issues budgets should be set aside for AI risk initiatives.

“Budget should be ring fenced for AI initiatives.” (Respondent 8)

Respondent 9 highlighted the need for obtaining buy-in from senior leadership.

“You need to show to EXCO that they can invest in AI from a risk point of view and the skilling of your current resources is important.” (Respondent 9)

Respondent 7 demonstrated that access to AI skills was a key barrier and highlighted the need to obtain the right AI skills to implement AI projects.

“Key issues included skills and experience. AI is relatively in its infant stage in risk management. AI is becoming the trend and many are trying to develop such tools to recreate the human journey digitally.” (Respondent 7)

Respondent 8 concurred with the skills issue to help advance AI initiatives.

“The first major challenge is obtaining budget, the second challenge is obtaining the right skills to build AI tools.” (Respondent 8)

To further unpack the AI skills’ challenge, respondents were asked to elaborate on whether the organisation had the AI skills necessary to implement AI solutions.

Respondent 9 indicated that although the organisation had AI skills, access to AI skills was a challenge.

“We do from a group perspective but we look at core and non-core functions. Because of financial resource limitations, we prioritise the core functions and higher investment instead of support functions. If a support function fails, the organisation will still exist as compared to a core business function.” (Respondent 9)

Respondent 15 further added that in accessing AI skills business functions obtained first priority.

“The organisation has access to skills but not all departments have access to the skills because of the priority given to business.” (Respondent 15)

Respondent 15 identified that in some instances AI skills resided within the technology function; however, capacity constraints made these skills inaccessible.

“Skills, we don’t have the skills within the department to drive such initiatives. We could go to technology; however, technology does not have capacity.” (Respondent 15)

Respondent 5 indicated that although there had been some improvement in building AI skills, improvement was still required.

“We are getting there, we have a big data team and some who have skills to write algorithms. However, there is room for improvement.” (Respondent 5)

Respondent 4 highlighted that there was access to AI skills; however, there was uncertainty around when the skills would be deployed.

“Yes, definitely. The skills side is there but it is a matter of knowing when it will be deployed into the business.” (Respondent 4)

Respondent 1 stated that there was some level of uncertainty as to whether or not the organisation had AI skills and there was limited buy-in to develop the skills within the risk function.

“I don't think so and you don't even get buy-in to build this capability. If you don't know the 'how' then it will be hard to implement and difficult to drive such [a] process if not provided with those skills.” (Respondent 1)

Respondents provided insights as to how the AI skills issue could be addressed.

Respondent 7 highlighted the need for cross-skilling between IT and risk to assist to understand each other's role and function to improve the success of AI projects.

“In terms of skills and experience you have two specific areas which is IT and risk. In order for this to be a success, IT would need to have a sense of what is risk management and risk a sense of what is technology or AI. It is a relationship where you need cross skilling.” (Respondent 7)

Respondent 9 indicated that obtaining buy-in from executive teams would encourage investment in AI skills.

“You need to show to EXCO that they can invest in AI from a risk point of view and the skilling of your current resources is important. Perform a training needs analysis and start putting training interventions.” (Respondent 9)

Respondent 8 recommended building internal AI capabilities within the risk management function.

“Build key data scientist capability within the risk function instead of sharing resources with business.” (Respondent 8)

Respondent 14 noted that to access AI skills, the skills were procured externally.

“We do to some extent and we generally use consultants.” (Respondent 14)

Respondent 12 believed that their respective organisation had AI and data-scientist skills.

“Yes, we have data scientists and AI skills who are a part of the company.” (Respondent 12)

Respondent 18 highlighted that AI and data-scientist capabilities had been built within the organisation.

“Yes, we have built a data science capability within the organisation.” (Respondent 18)

Respondent 20 indicated that although AI capabilities had been built up within the organisation, staff were encouraged to articulate use cases.

“Yes, we do, we have a platform internally to encourage staff to build and develop use cases.” (Respondent 20)

Respondent 12 raised an important point related to why AI skills were required, stating that the skills were needed to help a traditional Telco transition into becoming a Techco.

“It’s the company’s vision to have this capability in a centre of excellence. We need these skills as we move from a Telco to a Techco. Look at how Amazon and other 10x companies have used these skills to grow.” (Respondent 12)

Access to and availability of appropriate data were identified as another key barrier.

Respondent 8 noted that data issues concerned the poor quality of data and the complex system environment, which made it difficult to obtain data.

“Data was identified as a key challenge as data is not always clean, understandable and accessible across the organisation.” (Respondent 8)

Respondent 18 highlighted that data was not well understood which impeded AI implementations.

“Having access to data is not new to the industry but the industry has not realised that the data they have is the new oil. The biggest challenge is being able to make sense of the data.” (Respondent 18)

To mitigate data issues, Respondent 8 highlighted the need to implement an appropriate data governance framework to help improve data quality.

“Simplify the system landscape and implement an adequate data governance framework to improve data quality and governance.” (Respondent 8)

Respondent 10 highlighted the need for a single source of data for an overall view of the business landscape, which would make data easier to access and increase the chances of success.

“From a data perspective, we need a single source of data, data frameworks, risk needs to understand what is required and define use cases “(Respondent 10)

Respondent 15 stressed the need for AI models to be trained on quality data to avoid risks.

“Data needs to be accessible and clean to ensure that AI models are trained on quality data, to prevent issues later.” (Respondent 15)

Use cases also needed to be understood to ensure that data requirements were aligned to use cases.

“Data based on robust use cases should have been merged into the big data platform to have a central view of data that is aligned to the use case requirements. Data cleansing activities should have been performed to clean the data.” (Respondent 18)

Respondent 10 noted a challenge regarding the need for appropriate use cases, to be able to assist with machine training.

“Inadequate use case studies and trends to be able to teach the machine. Organisations are currently not ready for AI in risk management.” (Respondent 10)

Respondent 18 highlighted the ability to understand data to extract value from it as a difficulty.

“Understanding what triggers to pull and push to extract value from the data is an issue, especially when don’t have specific use cases.” (Respondent 18)

Respondent 12 believed that poor stakeholder buy-in contributed to AI implementation challenges.

“Executive understanding of early adoption of any technologies, such as the use of blockchain, machine learning or big data. Attempts to bring in this new technology, gets resistance as it’s seen as early investment which can be wasted. We tend to wait until the technology matures to see benefits, then there is a willingness open the wallet to budget for the technology. If you are ahead of the curve, it is difficult to get investment into new technologies.” (Respondent 12)

Respondent 15 also highlighted poor stakeholder buy-in, related to poor staff buy-in, as a barrier to AI implementation.

“During the roll out of the solution there were many soft issues such and lack of staff buy-in.” (Respondent 15)

Respondent 9 alluded to organisations' lack of preparedness for AI adoption as causing a barrier.

"Lastly organisational readiness level and transitioning which can be perceived as constraint or a limitation in making AI fully functional in an organisation." (Respondent 9)

Respondent 20 indicated that poor culture and lack of AI awareness might impede AI transformation.

"The biggest barrier is awareness of what AI can do. There are a lot of buzz words and a lot of people don't understand how this translates to their job and what does this mean to me." (Respondent 20)

Respondent 12 further added that the negative perception of AI was a barrier to its implementation.

"The fallacy that digital transformation will take away our jobs hampers AI advancement." (Respondent 12)

Respondents provided insights into what change management initiatives could be taken to address the above challenges.

Respondent 15 highlighted the need for an adequate change management plan to address issues.

"A proper change management plan to address culture issues." (Respondent 15)

Respondent 14 indicated that people needed to be involved early during AI initiatives.

"I would say, know what you want and get teams involved early so that they can also learn." (Respondent 14)

Respondent 6 highlighted the need for building trust in AI technology.

"I would say, one has to build trust in the AI technology so the applications can come with some accuracy." (Respondent 6)

Respondent 12 suggested creating an awareness of AI to drive the right culture towards AI.

“Buy in and support from key stakeholders is important, this can be done by educating stakeholders about new technologies such as AI, to see the benefits and value. We need to drive a digiterati culture, that’s a digitally minded culture.” (Respondent 12)

Respondent 9 indicated that to drive the right culture, support mechanisms should be in place for rewarding the correct behaviour regarding AI, improving the tone at the top and integrating digitilisation into the new way of doing business.

“With the readiness level – we must align with the organisational strategy. To drive a culture shift, we need to incentivise organisations to adopt AI, it’s a mind shift and the tone at the top. Digitisation is not a function it needs to be within our DNA to drive the right culture.” (Respondent 9)

Chapter 5: Discussion of the Findings

5.1 Introduction

This chapter provides a discussion of the findings of the study in relation to the literature review conducted. The discussion is structured according to the stated research propositions:

- Proposition 1: The increased adoption of digital technologies within the telecommunications industry in South Africa necessitates the integration of AI into the risk management function.
- Proposition 2: AI adoption can accelerate risk management processes to proactively manage exposure.
- Proposition 3: The implementation of AI solutions within a risk function requires an understanding of AI.

5.2 Proposition 1: The increased adoption of digital technologies within the telecommunications industry in South Africa necessitates the integration of AI into the risk management function

5.2.1 Risk management support

The study revealed that the risk management function within the telecommunications industry does not provide adequate risk support to business. This point of view was put forward by 50% of the respondents, who believed that the risk function does not provide adequate risk coverage as the function is still traditional and manual in nature, and not agile enough to match the agile nature of business. This makes the risk function unable to meet business demands. The finding echoes the need identified in the IRMSA survey that risk management should transition into a proactive function to manage the increasing volumes of data (IRMSA, 2021).

Forty per cent of the respondents believed that their risk management functions provide sufficient risk support by being proactive and agile. The finding demonstrates the need to be proactive while 10% of the respondents did not provide any related

comments. Inadequate risk support may have the potential to harm the business as the risk function assists the business plan and responds to potential risks. The findings align with the risk identified in the Protiviti risk profile survey that business is not well prepared to respond sufficiently to risks such as cyber risks (Protiviti, 2021).

5.2.2 Risk management technology adoption

In terms of the adoption of technology across the risk management function, 95% of the respondents were of the view that the risk function cannot implement risk management technologies at the same pace as business. Respondents indicated that the adoption of technologies such as AI in risk management has been a slow process since risk generally lags business owing to the prioritisation of business over the risk management function. The slow adoption process confirms the literature finding that the implementation of AI technologies in risk management processes can be sluggish (Lee et al., 2020). Five per cent of the respondents were unsure about the rate of technology adoption in the risk function in comparison to business.

This study finding corroborates the risk highlighted by the BDO telecommunications future risks survey that organisations are unable to adopt new technologies to improve internal processes (BDO, 2021). This may suggest that there is a technology and AI gap within the risk function.

Extending the discussion of the prioritisation of business mentioned above, respondents stated that business initiatives were prioritised over support functions, leading to the slow adoption of technology, including AI, within the risk function. The priority factor aligns with the BDO telecommunications future risks survey results, which indicate that the digitalisation of internal operational processes has not been prioritised (BDO, 2021). Respondents noted that insufficient budget allocations and risk technology being in its infancy phase of development contributed to the slow adoption of AI technology within the risk function.

A study by Jooman (2019) found that the influence of AI within South African internal audit functions is in its infancy, with a level of uncertainty related to when AI implementations will take place within the audit function. The current study findings

suggest that the risk management function is following a similar trajectory to internal audit from an AI implementation perspective.

To fill the AI technology adoption gap within the risk function, risk management has begun to focus on integrating risk controls into business processes, a concept defined as risk by design.

The study noted that although the development of AI within the risk function has been slow to take off, there have been positive impacts of the initial AI projects launched within specific risk functions. Existing AI initiatives within the risk function have enabled the function to identify and respond to specific risk types, such as fraud risk, quicker with limited manual intervention. Using current AI initiatives, the risk function has been able to realise savings, obtain efficiencies and add value to business and customers. The study echoes the findings of Lee et al. (2020), who state that organisations are deploying AI solutions to improve customer experience, obtain insights and create operational efficiencies.

Respondents agreed that existing AI solutions within the risk function have enabled the provision of real-time management of risk at the edge, highlighting use cases related to fraud risk and cyber security. This aligns to research performed by Aziz and Dowling (2018), which highlighted the use of AI within fraud and cyber risk use cases. The study also highlighted AI solutions related to SIM swap prevention.

5.2.3 Nature of risk management intervention – proactive vs reactive

It was important to understand the proactiveness or reactiveness of the risk management function within the telecommunications industry, to determine if there is a need to transition the risk function into a proactive risk function. The study revealed that 50% of the respondents believed their risk function to be reactive when managing risk. Their rationale was based on their risk function adopting manual processes and partial automation; inefficiencies related to risk operations; and limited human and financial resources. Aziz and Dowling (2018) identify partial automation and operational inefficiencies as reasons why companies invest in AI. This presents an opportunity for AI integration.

Although 45% of the respondents indicated that their risk function adopted both a reactive and proactive approach to risk management, the respondents indicated that still more progress is required to transition towards a proactive risk function.

It was noted that a proactive risk management approach was adopted for specific risk streams only, such as fraud and cyber risk. The cyber use case corroborates literature findings that AI solutions have enabled the proactive management of cyber security to limit risk exposures (Anwar & Hassan, 2017). Only 5% of the respondents believed their risk functions to be proactive in nature.

There is a need for the risk management function to transition towards becoming more proactive in nature. This specific research outcome is similar to the IRMSA survey (2021) finding that relates to the need for the risk management function to transition from a reactive risk management function to a more proactive function (IRMSA, 2021).

5.3 Proposition 2 – AI adoption has the ability to accelerate risk management processes to proactively manage exposure

5.3.1 Impact of Artificial Intelligence initiatives on risk management

This aspect of the study revealed that some risk functions have implemented AI solutions to help digitise and improve risk management process. The implemented AI solutions enabled the risk function to be more prepared to respond to and manage risk exposure and highlighted an improvement in response times. The improvement in response times correlates with the literature review, which revealed that AI has the ability to allow risk management to respond faster (Dialogic Innovation, 2020). This evidence demonstrates that AI can accelerate a risk management process or function.

However, two respondents noted that although AI has helped their risk function by improving risk response times, there is still room for improvement. A single respondent indicated that while AI enabled real-time risk engagement, response times were not improved. This finding contradicts the narrative that AI optimises processes (HBR, 2018). It is evident that the adoption of AI into risk management is not a straightforward process, and it may require time for the benefits of AI to be seen.

5.3.2 Criteria for identifying risk processes for Artificial Intelligence adoption

McKinsey (2017) identifies key criteria for successful AI implementation, such as appropriate use cases, availability of data, relevant tools, workflow integration and the right organisational culture (McKinsey & Company, 2017). The risk professionals interviewed for the study highlighted the following key criteria for identifying risk processes for AI adoption: adequate use cases, alignment to strategy, leveraging of automated processes, transformation of manual and repetitive processes, focus on customer and income-generating processes, integration of AI into high- and low-risk processes, practicality, knowledge of risk triggers and access to data.

There is some alignment between the literature review and the study; however, the study does provide additional points for consideration. These points are based on a risk management perspective, which includes strategic alignment; a focus on income-generating and customer processes owing to their high-risk nature; and the consideration of low or high risks and understanding of risk triggers. The success factors provided by the literature together with the additional points identified in the study findings provide a more customised view around how AI implementation can be successful and add value within the risk management function.

FERMA highlights that AI can be integrated into the ISO 31 000 risk management process, with specific focus on risk assessment, identification, analysis, monitoring and treatment, and the risk process (FERMA, 2019). The study listed risk identification, assessment, monitoring and reporting as key risk processes for AI integration, which meant that apart from reporting, the study echoed the suggestions made by FERMA. However, the study also revealed that the end-to-end risk management process needs to be transformed by the integration of AI. The end-to-end integration of AI into the risk management process will bring about more operational process efficiencies and better management of risk.

5.3.3 Use cases for Artificial Intelligence adoption

The literature review highlighted risk management use cases related to the adoption of AI, with use cases focusing on cyber risk, operational risk, fraud risk, credit risk, regulatory risk and market risk (Aziz & Dowling, 2018). However, the use cases were not specific to the telecommunications industry. The current study presented specific

telecommunications risk management use cases, which consisted of adopting AI to assess risk across customer onboarding processes; financial risks; cyber and fraud risk; and privacy and compliance use cases to identify and monitor risks. Although cyber risk and fraud risk already utilise AI to manage risk, further improvement of how AI is implemented in these use cases is required.

It was noted that the traditional Telco is transitioning into becoming a Techco. With this transition, there is a need to integrate AI into a broader array of use cases to manage risk, which include financial services use cases, insurance fraud risk, payment risk, fraudulent subscriptions, collections and understanding customer risk across both Telcos and Techcos. According to Lee et al. (2020), the development of technology pushes companies to implement AI solutions to improve and be competitive. This suggests that, as a Telco transitions into a Techco with increased technology and platforms, it is vital for the risk function to adopt AI.

5.3.4 Impact of Artificial Intelligence within the risk function

Respondents were of the view that the implementation of AI within the risk function has the ability to increase the output of the risk function. AI can drive the risk function to be more proactive and better able to predict and manage risk exposures, to add value to business. The idea of AI allowing a risk function to manage risk exposures is aligned to the insight provided by FERMA that AI can enable a risk function to be predictive and have a real-time view of potential exposures to improve risk responses. AI will improve decision making by having more visibility of and insight into risks (FERMA, 2019).

Biolcheva (2020) also revealed that using AI in risk management will provide the function with more insights, to make predictions with the aim of being forward looking (Biolcheva, 2020). This means that the study outcome is aligned to the narrative of AI being able to decrease risk exposures (Dialogic Innovation, 2020).

5.4 Proposition 3: The implementation of AI solutions within a risk function requires an understanding of AI

5.4.1 Understanding of Artificial Intelligence within the risk function

According to Forbes, it is important for business to have an understanding of concepts related to AI, such as knowledge of automation, deep learning and machine learning to be in a position to identify applications for AI integration (Forbes, 2021). During the study, 25% of the respondents reported that they had knowledge of AI, automation and big data, and indicated that they had a good understanding of automation and machine learning because of their involvement and experience in AI-related projects within the risk management function. Sixty per cent of the respondents highlighted that they were familiar with AI concepts while 15% indicated that their understanding of the concepts was limited. It is evident that the risk management function needs to increase its level of understanding of AI.

5.4.2 Artificial Intelligence implementation challenges

The study highlighted various AI-related challenges faced when implementing AI solutions within the risk management function. Key challenges related to budget constraints that prevent the risk function from investing in AI. Business priorities take precedence over risk function, with the result that the risk function may not be able to drive AI initiatives adequately.

Privacy laws have the potential to restrict the usage of data, which may prevent the risk function from extracting full value from AI solutions, as large amounts of data are required to train and refine AI solutions (UP, 2018).

Respondents noted that to address the budget constraints, it is vital to have buy-in from senior leadership to invest in AI from a capability perspective. In line with this, access to AI skills was viewed as a key barrier, with the risk function being unable to procure AI skills or leverage AI skills from within the organisation owing to the prioritisation given to revenue-generating activities or capacity issues related to the availability of AI staff. The decisions surrounding a plan of action to address the skills' gap may be complicated by AI efficiency potentially causing unemployment (BusinessTech, 2019).

The lack of AI skills has had a negative impact on the development of AI solutions within the risk function. According to Leo et al. (2019), the development of AI solutions

has been negatively affected by inappropriate AI skills. Improvement is required from an AI skills' perspective.

It was identified that there is a need to build AI skills' capability, which should be dedicated to the risk function to drive initiatives. In some instances, cross-skilling of technology and risk resources is necessary to better understand technology capabilities and the risk management process to identify AI opportunities. The study also noted that with the transition from a traditional Telco to a Techco, which has accelerated technology transformation, there is a need to develop AI skills within the risk function.

It is vital for the risk management function to develop AI skills, as a skills' gap has the potential to impact the risk function negatively as skill shortages can affect growth (UP, 2018).

According to Aziz and Dowling (2018), data that is held in silos can hamper the success of AI solutions as this prevents data from being structured in a meaningful way to be able to teach AI (Aziz & Dowling, 2018). During the study, data challenges related to data availability and access were highlighted. Data was reported as being of poor quality and of being scattered across the organisation, which prevent the risk function from appropriately understanding the data. For these reasons, the risk management function has a data-availability challenge (Aziz & Dowling, 2018).

Since data is a key factor for the teaching of AI to deliver results (UP, 2018), data gaps need to be addressed. To ensure that data-related gaps are addressed, the study identified a need for the establishment of well-defined data governance frameworks to drive data consistency across the organisation and to establish a single data source.

According to McKinsey (2017), the use of appropriate use cases is essential for the success of AI initiatives (McKinsey & Company, 2017). However, the study identified a gap in the risk management function in terms of appropriate use cases. This may result in AI solutions being trained on limited cases, which may promote inaccuracy as solutions need to be robustly tested to determine if they are performing as expected (Aziz & Dowling, 2018).

Respondents indicated that the potential benefit brought by AI to risk management was not generally understood. Issues were identified regarding a lack of stakeholder

buy-in to AI solutions and the risk function being unprepared from a readiness and awareness perspective to support AI development. This demonstrates a key cultural barrier that could potentially hinder the success of an AI solution (McKinsey & Company, 2017). It is therefore vital for risk management functions to drive the right culture related to AI solutions with appropriate change management plans that involve individuals early in the development process to build trust in AI solutions.

Chapter 6: Conclusions and Recommendations

6.1 Introduction

The following chapter provides the conclusions of the study by discussing how the research findings meet the research objectives and confirm the research propositions. The chapter then makes recommendations that arise from these conclusions. The chapter concludes with the contribution of the study and suggestions for future research.

6.2 Conclusions pertaining to the main research objective

The main research objective of this study was to examine the effect of AI technologies on a risk function, and their ability to transform the risk function into a proactive function within the South African telecommunications industry.

The adoption of technology within the telecommunications industry is bringing more complexity to the industry and increasing the need for risk management to provide adequate risk support. The increased adoption of technology inherently exposes a business to more risk and increases the demand for proactive risk management. However, the study highlighted that risk management is unable to provide support to business fully because of challenges such as budget constraints, slow AI technology adoption and business initiatives taking priority over risk management. These challenges have the effect of pushing the risk management function to be reactive in nature, with only an element of proactiveness.

Evidence from initial use cases suggests that AI can help a risk function move forward towards becoming proactive as it enables the risk function to move away from the subjective nature of risk management towards decisions being driven by data (FERMA, 2019). This suggests that the telecommunications risk management function will benefit from transforming from traditional risk management approaches by introducing AI technologies within the risk function to drive proactive risk management.

These conclusions confirm Proposition 1: The increased adoption of digital technologies within the telecommunications industry in South Africa necessitates the integration of AI into the risk management function.

6.3 Conclusions pertaining to Research sub-objective 1

Research sub-objective 1 sought to understand what risk applications AI can be integrated into.

The study found that AI can be integrated into a number of risk applications, with the first being risk management processes. The integration of AI into risk management processes can enable the risk management function to proactively respond to risks and potentially limit risk exposure.

Secondly, the study demonstrated that integrating AI into specific applications improves risk response times. The study specified particular use cases and risk management processes for the adoption of AI. The use cases provide a list of opportunities that can be investigated and integrated with AI for improvement. Use case opportunities include customer onboarding, financial, compliance, cyber, subscription fraud, billing, and collections processes. Refer to section 4.3.3 and 4.3.4 for additional details.

The third risk application arises from a company's transition from a Telco to a Techco. With this transition there is a need to utilise AI within the risk process as the organisation becomes more digitally driven and faces new risk types that require more digitally enhanced risk management tools such as AI. The integration of AI prompts the risk function to be more proactive, and able to cope with the volume of risk and new risk types.

To improve the chances of implementing AI within risk function applications, the study highlighted key criteria to identify the appropriate risk management processes for AI adoption within the risk function of a telecommunications company. Some of these criteria are alignment to strategy, transformation of manual and repetitive process, focus on customer and income-generating processes, and integration of AI into high- and low-risk processes. Refer to section 4.3.2 for additional details

The study revealed that existing AI initiatives have been beneficial to the risk function and provide specific risk management criteria to be included in AI adoption projects to improve the impact of AI and increase the chances of success. Refer to section 4.3 for additional details. This validates Proposition 2: AI adoption has the ability to accelerate risk management processes to proactively manage exposure.

6.4 Conclusions pertaining to Research sub-objective 2

Research sub-objective 2 aimed to investigate the barriers surrounding the adoption of AI technologies within a risk function.

A major barrier to the adoption of AI within a risk management function in the telecommunications industry relates to budget constraints, which prevent further investment in the procurement of AI skills. Budget constraints have been caused by senior managers who are doubtful about investing in AI. Access to specialised AI skills within the risk management function is a challenge that has been brought about by business being prioritised first or by capacity constraints in existing AI-skilled resources. The lack of a central source of data creates data accessing and quality issues. Refer to section 4.4.2 for additional details.

Risk management use cases are not adequate for sufficiently training the risk function in AI technologies. A lack of stakeholder buy-in was also identified as an AI barrier, with a negative impact on the ability to drive the right digitally-minded culture. The study also noted that in the regulatory risk area, privacy requirements have the ability to restrict data usage.

The study also revealed that only 25% of the respondents understood the concepts related to AI, thereby indicating a knowledge gap which is potentially hampering the risk function's ability to roll out AI-related projects. Refer to section 4.4.1 for additional details.

It is important to note that the majority of the challenges identified can be attributed to no or limited understanding of AI. This means that change management interventions are required to improve the current mindset to encourage the adoption of AI.

Lastly, the understanding of AI within risk management should not be underestimated, as a comprehensive understanding of AI will assist the function to identify appropriate AI applications and potential challenges, to curb issues for a greater chance of success regarding AI implementations. These conclusions are aligned to Proposition 3: The implementation of AI solutions within a risk function requires an understanding of AI.

6.5 Recommendations

The risk function within the telecommunications industry is still very manually intensive and traditional. Although successful AI solutions have been deployed within the risk function, there is still a gap in the implementation of AI. The following recommendations are made with the aim of reducing this gap:

1. The telecommunications industry is currently adopting new technologies to evolve operations to become more digitally driven and build new digital services that are aligned to a Techco. This transformation will inherently expose organisations to additional risks; however, it is up to the risk management function to provide adequate support to de-risk and manage these risk exposures proactively. Therefore, risk management functions within the industry should develop technology road maps that include AI to transform the risk function.
2. To address AI adoption challenges within the risk function, the function should establish change management initiatives to help drive awareness and obtain stakeholder buy-in to create the desired culture that supports the development of AI. The intervention should also focus on senior leadership within the risk function to enable it to understand the value-add that AI will bring to the risk management function, in an attempt to improve investment in risk AI.
3. Each risk management function should ideally start to build its own AI skills' capability within the risk function, as this will reduce the dependency on sourcing AI skills from business, to help focus and drive transformation of the risk function. Ideally the risk function should leverage off existing big data platforms within the organisation to access data to build AI solutions.
4. Once there is a good understanding of AI and the capabilities of AI, the risk function should develop suitable use cases for AI adoption. This will help contextualise the problem that AI needs to solve, which in turn will assist risk management to accelerate transformation. Risk functions should identify use cases that have the potential to be a quick and successful win, as this will help build trust and confidence in the technology.

6.6 Contribution of study

Previous research has focused mainly on risk management functions within the financial sector (Aziz & Dowling, 2018). The current study contributes to the study of risk management by providing insights into the adoption of AI within the risk management function from the perspective of the telecommunications industry.

AI initiatives implemented within the risk function have predominately been focused on fraud risk and cyber risk use cases. These initiatives have improved the risk function's response times and enabled the risk function to respond to risk exposures proactively, by responding to and managing risk in real time at the edge, in this way demonstrating the effect of AI on the risk management function, with the ability to transform the risk function. However, considering that the telecommunications industry is currently in a period of transition where Telcos are becoming Techcos, that the adoption of technology into the risk management function is in its infancy phase and that the risk function is still very traditional in nature. The Telco transitioning has provided insights into how the business and risk management environment is changing with development of non-traditional Telco services, which highlights the need for risk management functions to transform with technology, such as AI.

Earlier research focused predominantly on the adoption of AI into cyber risk, fraud risk, market risk and credit risk use cases, across risk functions from the financial services industry (Aziz & Dowling, 2018). The current study extends this research by providing insights into the adoption of AI from a telecommunications risk management perspective. Although fraud and cyber risk solutions have been deployed, the study identified additional use cases for AI adoption, which include financial risk processes, customer onboarding risks and compliance use cases to identify and monitor risks.

In relation to the ISO 31 000 risk management process, the study lists key processes within the risk management process that can be integrated with AI. The risk processes include risk identification, risk assessment, risk monitoring and reporting as key processes for AI adoption. The end-to-end transformation of risk management process with AI is also useful as the entire risk process can be transformed with AI to gain operational efficiencies, be more proactive and overall manage risk exposure better.

6.7 Suggestions for further research

The study highlighted the transformation of traditional telecommunications companies into Techcos, where telecommunications companies venture into new businesses such as insurance, payments and content services that involve offering payment solutions, insurance services, content subscription services, IoT services, cloud services and marketplace platforms such as a Super App.

It is therefore suggested that further research be conducted to understand the impact of the telecommunications transformation on the risk management function to determine how the risk function should deal with the transition.

References

- Anwar, A., & Hassan, S. I. (2017, March 1). Applying artificial intelligence techniques to prevent cyber assaults. *International Journal of Computational Intelligence Research*, 13(5), 883–889. Retrieved from https://www.ripublication.com/ijcir17/ijcirv13n5_19.pdf
- Aziz, S., & Dowling, M. (2018). AI and machine learning for risk management. *SSRN Electronic Journal*, 1–18. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3201337
- BDO. (2021, February 4). *BDO's 2021 telecommunications risk factor survey*. BDO South Africa . Retrieved from: <https://www.bdo.co.za/getattachment/Insights/2021/Advisory/2021-Telecommunications-Risk-Factor-Survey/2021-telecommunications-risk-factor-survey-final.pdf.aspx>
- Biolcheva, P. (2020). Trends in the development of risk management. *Trakia Journal of Sciences*, 18, 417–421.
- BusinessTech. (2019, April 26). *South Africa's massive jobs challenge: Balancing automation and unemployment*. Retrieved from: <https://businesstech.co.za/news/technology/313572/south-africas-massive-jobs-challenge-balancing-automation-and-unemployment/>
- Chandrinou, S. K., Sakkas, G., & Lagaros, N. D. (2018). AIRMS: A risk management tool using machine learning. *Expert Systems with Applications*, 105, 34–48.
- Creswell, J. W. (2014). *Research design*. Sage Publications.
- Dialogic Innovation. (2020, June 17). *Managing AI use in telecom infrastructures: Advice to the supervisory body on establishing risk-based AI supervision*. Utrecht: Dutch Radiocommunications Agency. Retrieved from: <https://rbekkers.ieis.tue.nl/resource/BRC194-2020-vdvorst-ai-telecom.pdf>
- expert.ai. (2020, May 6). *What is machine learning? A definition*. Retrieved from: <https://www.expert.ai/blog/machine-learning-definition/>
- Federation of European Risk Management Associations (FERMA). (2019, 12 04). *Artificial Intelligence (AI) applied to risk management*. Retrieved from:

<https://www.ferma.eu/publication/artificial-intelligence-ai-applied-to-risk-management/>

Harvard Business Review (HBR). (2018). *Artificial intelligence for the real world*.

Retrieved from: <https://www.kungfu.ai/wp-content/uploads/2019/01/R1801H-PDF-ENG.pdf>

IBM Cloud Education. (2020, June 3). *Artificial Intelligence (AI)*. Retrieved from:

<https://www.ibm.com/za-en/cloud/learn/what-is-artificial-intelligence>

Institute of Risk Management South Africa (IRMSA). (2021, April 1). *Resources*.

Retrieved from: <https://irmsa-risk-report.web.app/riskreport2021/>

International Organization for Standardization (ISO). (2009, May 1). *Risk*

management — Principles and guidelines (ISO Standard No. 31000:2009).

Retrieved from: <https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en>

Jooman, S. A. (2019, March 1). *Internal audit and artificial intelligence*.

Johannesburg. Retrieved from: https://grippadvisory.co.za/wp-content/uploads/2020/08/TL-AI-and-IA-Part-1-of-2_Final.pdf

Lardi, K. (2021, January 26). *Understanding the value of artificial intelligence*

solutions in your business. Forbes. Retrieved from:

<https://www.forbes.com/sites/forbesbusinesscouncil/2021/01/26/understanding-the-value-of-artificial-intelligence-solutions-in-your-business/?sh=6ddea238657f>

Lee, M., Floridi, L., & Denev, A. (2020). Innovating with confidence: Embedding

governance and fairness in a financial services risk management framework.

Berkeley Technology Law Journal, 34(2), 1–19.

Leo, M., Sharma, S., & Maddulety, K. (2019, March 5). Machine learning in banking

risk management: A literature review. *Risks*, 7(9), 1–22.

doi:10.3390/risks7010029

McKinsey & Company. (2017). *Artificial Intelligence: The next digital frontier?*

McKinsey Global Institute. Retrieved from:

<https://www.mckinsey.com/~media/mckinsey/industries/advanced%20electronics/our%20insights/how%20artificial%20intelligence%20can%20deliver%20r>

eal%20value%20to%20companies/mgi-artificial-intelligence-discussion-paper.ashx

Oracle. (2020, June 1). *Big Data*. Retrieved from: <https://www.oracle.com/za/big-data/what-is-big-data/>

Protiviti. (2021, March 1). *Top risks for 2021 and 2030 – Technology, media and telecommunications industry perspectives*. Retrieved from: doi:<https://www.protiviti.com/US-en/insights/top-risks-2021-and-2030-technology-media-and-telecommunications-industry-perspectives>

Protection of Personal Information Act (POPI Act), Act 4 of 2013. (2021, January 26). Retrieved from: <https://popia.co.za/>

Salesforce. (2021, May 1). *What Is digital transformation?* Retrieved from: <https://www.salesforce.com/eu/products/platform/what-is-digital-transformation/>

Statistics Solutions (2021, July 1). *What is transferability in qualitative research and how do we establish it?* Retrieved from: <https://www.statisticssolutions.com/what-is-transferability-in-qualitative-research-and-how-do-we-establish-it/>

University of Pretoria (UP). (2018, November 19). *Artificial intelligence for Africa: An opportunity for growth, development, and democratisation*. Pretoria: University of Pretoria. Retrieved from: https://www.up.ac.za/media/shared/7/ZP_Files/ai-for-africa.zp165664.pdf

APPENDIX A: Participant information sheet for interviews

Dear participant

My name is Nitesh Ramatar and I am a Masters student in Master of Management in the field of Digital Business at the University of the Witwatersrand, Johannesburg. As part of my studies, I have to undertake a research project. I am exploring Artificial Intelligence-driving the transformation of risk a management function in the South African Telecommunications Industry. The research will be conducted under the supervision of Dr Manessah Alagbaoso. The aim of the research is to understand how AI technologies can be used to transform risk functions within the telecommunications industry in South Africa.

Your support by participating in research study would be much appreciated. I would like to invite you to a one-hour interview. The interview will be scheduled according to your availability and all data related to the interview will be kept confidential. Please note that your participation is voluntary and you will not receive any direct benefits from participation.

If you have any questions, feel free to contact me. This study will be written up as a research report which will be available online through the university library website.

Yours sincerely,

Researcher:

Nitesh Ramatar 1810397@students@wits.ac.za

Supervisor:

Dr Manessah Alagbaoso

APPENDIX B: Consistency matrix

Objective #	Research objective	Proposition	Data source and type	Analysis	Literature review
1	To examine the effect of AI technologies on a risk function, and its ability to transform the risk function into a proactive function within South African telecommunications industry	The increased adoption of digital technologies within the Telecommunications industry in South Africa necessitates the integration of AI into the risk management function.	Qualitative (interviews)	Qualitative: Thematic analysis	Aziz, S., & Dowling, M. (2018). Biolcheva, P. (2020). Chandrinou, S. K., Sakkas, G., & Lagaros, N. D. (2018). ISO. (2009, May 1). Lee, M., Florida, L., & Denver, A. (2020). Anwar, A., & Hassan, S. I. (2017, March 1). UP. (2018, November 19).

Objective #	Research objective	Proposition	Data source and type	Analysis	Literature review
2	To understand what risk applications AI can be integrated into.	AI adoption has the ability to accelerate risk management processes to proactively manage exposure.	Qualitative (interviews)	Qualitative: Thematic analysis	Aziz, S., & Dowling, M. (2018). Biolcheva, P. (2020). Chandrinou, S. K., Sakkas, G., & Lagaros, N. D. (2018). ISO. (2009, May 1). Lee, M., Florida, L., & Denver, A. (2020). Anwar, A., & Hassan, S. I. (2017, March 1).

					UP . (2018, November 19). McKinsey & Company. (2017). FERMA. (2019, 12 04)
--	--	--	--	--	---

Objective #	Research objective	Proposition	Data source and type	Analysis	Literature review
3	To investigate the barriers surrounding the adoption of AI technologies within a risk function.	The implementation of AI solutions within a risk function requires an understanding of AI.	Qualitative (interviews)	Qualitative: Thematic analysis	Aziz, S., & Dowling, M. (2018). Biolcheva, P. (2020). Chandrinou, S. K., Sakkas, G., & Lagaros, N. D. (2018). Jooman, S. A. (2019, March 1).

					Lee, M., Florida, L., & Denver, A. (2020). Anwar, A., & Hassan, S. I. (2017, March 1). UP . (2018, November 19).
--	--	--	--	--	---

APPENDIX C: Interview guide

To understand what risk applications AI can be integrated into	
No	Question
1	How would you describe the current risk management function, in terms of risk identification, assessment and monitoring? Example as proactive or reactive, please elaborate?
2	Is the risk function able to keep up with business, in terms of technology implementation and adoption to improve processes?
3	In general, is the risk function able to provide adequate risk assurance to businesses evolving needs, please elaborate on your reasoning?
4	Are you aware of technologies deployed within the risk function to automate and improve risk management processes? examples include the identification, assessment, monitoring etc.? please can you elaborate?
5	Are you familiar with artificial intelligence (AI), automation and machine learning? Please elaborate?
6	With your understanding of AI and risk management what criteria would use to determine which risk management processes can be enabled with AI? ISO process?
7	Which risk management processes do you think can be enabled with AI technologies?
8	Does your risk management function or process make use of AI technologies?
9	Please can you elaborate on which applications can be integrated with AI to move towards real-time identification of and monitoring or risk management?
To investigate the barriers surrounding the adoption of AI technologies within a risk function	
1	In the past, has your risk function tried to implement any AI technologies to improve the risk management process?
2	Please can you elaborate and describe any challenges faced when implementing AI solutions?
3	How could the challenges be mitigated?
4	Does your organisation have access to AI skills to implement AI solutions?

5	Does the organisation's technical infrastructure support the development of AI solutions, in terms big data and computer processing power?
6	Who is responsible within the organisation to drive AI solutions, is it the technology department or business owner? Is this approach adequate?
To examine the effect of AI technologies on a risk function, and its ability to transform the risk function into a proactive function within South African telecommunications industry	
1	What effect has AI had on your risk function?
2	Has the use of AI in risk management improved your functions response time and allows risks to be better managed, please can you elaborate?
3	Will the use of AI in risk management allow the function to be more proactive in nature? please elaborate?

APPENDIX D: Ethics approval

Graduate School of Business Administration
University of the Witwatersrand, Johannesburg



Wits Business School Ethics Committee
Constituted under the University Human Research Ethics Committee (Non-Medical)

Ethics Clearance Certificate

Ethics protocol number: WBS/DB1810397/418

This certificate is only valid with a legitimate ethics protocol number and signed by the Researcher (below)

This certificate is only valid if accompanied by formal permission from the relevant stakeholder(s).

Project title Artificial Intelligence-driven transformation of the risk management function in the South African telecommunications industry

Investigator / Researcher Mr Nitesh Ramatar

Nature of Project MM (Digital Business)

Decision of the Committee Approved, provided stakeholders and participants are guaranteed confidentiality.

Issue Date of Certificate 2021-08-18

Expiry date Date of submission of the project report

Chairperson Prof Anthony Stacey
☎ +27 11 717 3587
☎ +27 82 880 4531
✉ anthony.stacey@wits.ac.za

Declaration by Researcher

One copy must be signed by the Researcher and returned to the Chairperson of the Wits Business School Ethics Committee.

I fully understand the conditions under which I am 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 undertake to resubmit the protocol to the Committee.

Signature

13 / 02 / 2022

Date: