

https://dspace.org/

Corporate governance of robotic process automation by South African firms

Nortje, Anri

2023
https://hdl.handle.net/10539/37199

Downloaded from a DSpace repository. https://dspace.org/

Corporate governance of robotic process automation by South African firms

Anri Nortje

A research report was 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

Supervised by Dr Lucienne Abrahams

October 2022

KEYWORDS

Robotic process automation, RPA, corporate governance, cyber security, data protection, digital ethics

ABSTRACT

Traditional corporate governance policies and principles do not make provision for the implications of new technologies, like robotic process automation, on digital business. Without the appropriate governance of technologically-enabled advancements, firms are exposed to new threats and face increased vulnerabilities. Using constructivism, this study aimed to understand which governance principles firms in South Africa should have in place for the use of robotic process automation. The study finds that the governance of robotic process automation depends on (i) digital governance and risk management, (ii) cybersecurity and data protection, and (iii) digital business ethics considerations that firms need to address when they deploy robotic process automation software. Based on the findings and the data analysis, the study formulates a model for the governance of robotic process automation called *"an expanded model for RPA governance in South African digital business".* From this model, the study concludes with seven governance principles, proposed by the researcher, to assist South African firms with the governance of robotic process automation.

DECLARATION

I, Anri Nortje, declare that this research report is my work except for the references and acknowledgements indicated. It is submitted in partial fulfilment of the requirements for the degree in 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 other universities.

Name: Anri Nortje Signature:  Signed at: Boksburg, Gauteng

DEDICATION

To my ever-loving and supportive husband, I am truly thankful for your constant support and encouragement during my pursuit of knowledge.

To the Institute of Directors South Africa, with the wish that this work can advance the inclusion of RPA governance in corporate governance training for the digital business environment.

ACKNOWLEDGEMENTS

I would like to thank the following people, without whom, I would not have been able to finish this research. To Wits Business School for driving knowledge and innovation in digital business. Thank you to my supervisor, Dr. Lucienne Abrahams for providing me with invaluable guidance throughout my research. To the people who participated in this research, thank you, without your knowledge and expertise this research would not have been possible. Also, to my employer, thank you for allowing me the time to finish my research. Finally, I would also like to thank my parents who gave me the ability to follow my dreams and for teaching me to never give up on what I want to achieve.

TABLE OF CONTENTS

ABSTRACT ..... *ii*

DECLARATION ..... *iii*

DEDICATION ..... *iv*

ACKNOWLEDGEMENTS ..... *v*

LIST OF TABLES ..... *ix*

LIST OF FIGURES ..... *x*

LIST OF ACRONYMS ..... *xi*

Chapter 1: An introduction to the governance of RPA *1*

1.1 Chapter introduction **1**

1.2 Research problem statement **1**

1.3 Purpose of the study **1**

1.4 Main research question **2**

1.4.1 Research sub-questions 2

1.5 Elements of RPA governance **2**

1.6 Significance of the study **4**

1.7 Delimitations of the study **4**

1.8 Chapter outline **5**

Chapter 2: Literature overview on the governance of RPA *6*

2.1 Chapter introduction **6**

2.2 Key elements of the study **6**

2.3 IT governance and risk management **6**

2.3.1 The role of the board in ITG 6

2.3.2 ITG structures 7

2.3.3 ITG risks and challenges 8

2.3.4 ITG theories 9

2.3.5 RPA's impact on ITG and risk management 11

2.3.6 Analytical perspective 11

2.4 Cybersecurity and data protection **12**

2.4.1 The role of the board in ensuring cybersecurity 12

2.4.1.1 Cybersecurity governance 12
2.4.2 Data protection governance 14
2.4.3 Data protection in South Africa 15
2.4.4 RPA's impact on cybersecurity and data protection 17
2.4.5 Analytical perspective 17
2.5 Digital ethics 17
2.5.1 What does digital ethics entail? 17
2.5.2 Cybersecurity ethics 17
2.5.3 RPA's impact on digital ethics 19
2.5.4 Analytical perspective 20
2.6 Summation of current literature on RPA governance 20
2.7 Rudimentary model for the governance of RPA by South African firms 20
Chapter 3: Using constructivism to develop a model for the governance of RPA 22
3.1 Chapter introduction 22
3.2 Research approach 22
3.3 Research design 22
3.4 Data collection methods 23
3.5 Population and sample 23
3.6 Research instrument 25
3.7 Procedure for data collection 25
3.8 Data analysis and interpretation 25
3.9 Limitations of study 28
3.10 Ethical considerations 28
Chapter 4: Study results on the governance of RPA 30
4.1 Chapter introduction 30
4.2 Findings relating to how ITG and risk management are affected by implementing RPA 30
4.2.1 Effect of RPA on ITG structures 30
4.2.2 ITG challenges due to RPA adoption 32
4.2.3 The effects of RPA on risk management 34
4.3 Findings relating to ways in which RPA affects cybersecurity and data protection 36
4.3.1 Cybersecurity considerations for the adoption of RPA 36

4.3.2 Data protection and data security considerations when firms use RPA 37
4.3.3 Data protection or cybersecurity challenges faced by firms 40
4.4 Findings relating to how South African firms can ethically manage the digitalisation process when adopting RPA 40
4.4.1 Ethical considerations when firms deploy RPA 40
4.4.2 The effect of RPA on the employment of firms 41
Chapter 5: An expanded model for the governance of RPA 45
5.1 Chapter introduction 45
5.2 The adoption of RPA and its effect on ITG and risk management 45
5.2.1 The effect of RPA on ITG structures 45
5.2.2 The effect RPA has on risk management 47
5.3 The adoption of RPA and its effect on affect cybersecurity and data protection 49
5.3.1 The effect of RPA on cybersecurity management 49
5.3.2 The effect RPA has on data protection 52
5.4 The adoption of RPA and how South African firms can ethically manage the digitisation process when adopting RPA 54
5.5 The expanded model for the governance of RPA by South African firms 57
Chapter 6: Governance principles of RPA 62
6.1 Chapter introduction 62
6.2 Corporate governance principles for using RPA by firms in South Africa 62
6.3 Recommendations for future research 63
References 65
APPENDIX A: Codes consolidation matrix 69
APPENDIX B: Participant information sheet 78
APPENDIX C: Informed consent 79
APPENDIX D: Interview guide 80
APPENDIX E: Ethics approval 81

LIST OF TABLES

Table 1: Key facets boards should consider ensuring ITG 9
Table 2: Comparison of data privacy principles and POPIA 16
Table 3: Participant profiles..... 24
Table 4: Sub-categories classified per main category 28

LIST OF FIGURES

Figure 1: M-TISM model for cybersecurity management 13
Figure 2: Five cybersecurity ethics principles 19
Figure 3: A rudimentary model for RPA governance by South African firms 21
Figure 4: Elements of ITG concerning the governance of RPA 46
Figure 5: Elements of risk management concerning the governance of RPA 48
Figure 6: Elements of cybersecurity concerning the governance of RPA 50
Figure 7: Elements of data protection concerning the governance of RPA 52
Figure 8: Ethical considerations in relation to the governance of RPA 54
Figure 9: Five cybersecurity ethics principles (adapted) 57
Figure 10: Digital governance and risk management elements for the governance of RPA 58
Figure 11: Cybersecurity and data protection measures for the governance of RPA 59
Figure 12: Digital ethics for the governance of RPA 60
Figure 13: An expanded model for RPA governance in South African digital business 61

LIST OF ACRONYMS

CDR	Corporate Digital Responsibility
COBIT	Control Objectives for Information and Related Technology
COVID	Coronavirus Disease
ERP	Enterprise Resource Planning
HREC	Health Research Ethics Committee
IT	Information Technology
ITG	Information Technology Governance
M-TISM	Modified Total Interpretive Structural Model
NCPF	National Cybersecurity Policy Framework
OECD	Organisation for Economic Co-operation and Development
POPIA	Protection of Personal Information Act 4 of 2013
RPA	Robotic Process Automation
WBS	Wits Business School

Chapter 1: An introduction to the governance of RPA

1.1 Chapter introduction

Working with robotic process automation (RPA) within corporate finance in all sectors of South Africa has brought to light the lack of formal governance guidelines for all firms. Based on the experience of the researcher, this research aims to determine what governance guidelines South African digital business should have in place when they deploy RPA. There are several firms in South Africa that are predominant to using RPA including, firms in manufacturing, banking, and financial services, investments, software development and retail.

1.2 Research problem statement

The current body of literature does not adequately address the policies and procedures that need to be in place to ensure good corporate governance when a firm adopts RPA. Traditional governance policies and practices do not make provision for these new technologies. In this study, corporate governance in the context of RPA refers to the following three elements (i) IT governance (ITG) and risk management, (ii) cybersecurity and data protection, (iii) business ethics in the process of digitalisation of RPA by firms in South Africa. Without appropriate governance, organisations are exposed to threats and new/or increased vulnerabilities. These threats include ITG and risk management as well as in cybersecurity and the mishandling of data (including personal information) by individuals and firms. The Board of Directors needs to ensure that the digitalisation process is done in a controlled manner and ethically in conjunction with their traditional duties.

1.3 Purpose of the study

This constructivist study aims to understand and develop the corporate governance principles that need to be applied when firms in South Africa use RPA. At this stage in the research, the aim is to contribute to the literature by investigating the impact RPA has on corporate governance and what policies and procedures need to be in place to ensure good governance. This study aims to provide data and analysis on ITG and risk management, cybersecurity and data protection, and the necessary ethical considerations and how these are impacted by using RPA, derived from the South

African private sector context. This study will also explore the best policies and procedures that support good corporate governance and what needs to be in place when firms adopt RPA technologies. Corporate governance is a well-researched topic with many interconnected and complex elements. This study has a clear focus only on the use of RPA and its impact on corporate governance to help develop policies and procedures which firms can use adapt governance measures to include the specific use of RPA.

1.4 Main research question

How should corporate governance policies and procedures adapt in relation to the adoption and use of RPA by South African firms?

1.4.1 Research sub-questions

- How is ITG and risk management impacted by implementing RPA?
- In which way does the use of RPA affect cybersecurity and data protection?
- How can a South African firm ethically manage the digitalisation processes when adopting RPA?

1.5 Elements of RPA governance

RPA is a digital solution that provides a methodology to perform routine and repetitive business tasks through automation (Huang & Vasarhelyi, 2019). Lowes et al. (2017) describe RPA as the *"repeatable and predictable interactions"* of a program with multiple IT applications and programs while using pre-programmed and predefined rules to make decisions. RPA is used in South African capital markets, retail banking, wealth and asset management, telecoms, insurance, retail, manufacturing, and healthcare (Rutaganda et al., 2017; Yuvaraja, 2018). Maroun and Cerbone (2020) found that good corporate governance can better financial performance and generate higher market values for firms.

A study conducted by Syed et al. (2020) on 145 research papers found that the benefits of using RPA include an increase in operational efficiency and the quality of service delivery. Rutaganda et al. (2017) add that the use of RPA can improve compliance due to the improved traceability of transactions by using process logs and

documentation, while RPA simplifies operations and reduces costs. RPA ultimately improves accuracy, consistency, reliability, scalability, reporting quality and transparency (Yuvaraja, 2018).

The Institute of Directors South Africa (IODSA) describes corporate governance as managing a firm ethically and effectively while leading the organisation to achieve an ethical corporate culture, good performance, apply adequate controls and ensure legitimacy (IODSA, 2016). South African corporate governance policies and procedures, notably the King IV® report for corporate governance in South Africa (King IV®), superficially address IT governance but do not guide robotic process automation adoption. Principle 12 of the King IV® report only guides the use of technology by firms in South Africa by stating that technology should be implemented to support the firm's strategic objectives (IODSA, 2016).

ITG forms an integral role of corporate governance, and it is the responsibility of the top management of the firm (Bergeron et al., 2015). Bergeron et al. (2015) expand on this by stating that ITG contains the decision rights and an accountability framework for individuals to encourage the desirable use of IT systems within the firm and ensure that the set IT objectives and goals are met.

Cybersecurity, regulated by the National Cybersecurity Policy Framework (NCPF), is how a firm protects data assets from cybercriminals. Cybersecurity becomes a concern when deploying RPA as these technologies are given access to systems to perform tasks which exposes a firm to additional cybersecurity risks. The second element of this study includes data protection which is two-fold; it is the protection of personal information regulated by the Protection of Personal Information Act 4 of 2013 (POPIA) and business information and data assets. A critical question that needs to be answered is: do directors have sufficient knowledge, insight, and perspectives on ITG and the risks that new technologies may pose to a business? This is vital due to the current digital environment with a renewed focus on rapidly changing technologies and their challenges for modern firms. The importance of data protection is brought forth by the exponential advances in technology and the increasing ability of firms to gather, process and store personal data of individuals (de Bruyn, 2014). Individuals are leaving digital footprints on the internet by using their phones and personal computers, thereby increasing their vulnerability and increasing the ability of firms to

use and process data without a person's knowledge or consent (de Bruyn, 2014). Firms are making more use of cloud computing services that improve the data processing ability of the firm but expose their privacy risk if the country where the service is hosted does not meet the data privacy requirements of the country in which the firm operates (de Bruyn, 2014).

Lastly, digital ethics is the moral principles or rules that guide behaviour to minimise the risk of potential harm while ensuring that the maximum benefit is derived from the process (Whiting & Pritchard, 2017). Corporate digital responsibility (CDR), according to Orbik and Zozuľaková (2019), is the ethical consideration across all levels of a firm, ensuring the socially responsible transformation for an increasingly digital workforce and processes. In this paper, digital ethics and CDR are used interchangeably and refer to the ethical conduct required for a firm in digital transformation or a firm that has reached digital maturity.

1.6 Significance of the study

Theoretically, this research adds to the body of literature on the role of RPA and how it affects corporate governance in South Africa. Specifically, this research shows how ITG, and risk management are impacted when RPA is introduced to firms and the effect that RPA has on the cybersecurity and data protection protocols in place. Finally, this research also shows how to ethically implement RPA solutions by guiding the policies and procedures that should be in place to ensure good governance when South African firms adopt and use RPA software. In practice, this research provides corporate leaders with a frame of reference for policies and procedures that need to be in place, supporting good governance when RPA is introduced to everyday business processes.

1.7 Delimitations of the study

This study is a qualitative study on the impact that RPA has on ITG and risk management, cybersecurity and data management, and the ethical considerations for the digitalisation of business processes. The aim is to determine what policies and procedures result in good governance when firms implement and use RPA. Further research can be conducted on elements of corporate governance not covered in this

study (i.e., internal control, operational risks, auditing, reporting, sustainability, skills development, compliance, and applicable regulations) and how the use of RPA impacts these elements.

1.8 Chapter outline

Chapter 1 gives an overview of this paper by outlining the problem statement, purpose, background, and significance of this study. This chapter highlights the delimitations of the study while also outlining the main research questions and the relevant sub-questions.

Chapter 2 provides an overview of the literature on the main research topics, including ITG and risk management, cybersecurity and data protection, and the ethical digitalisation of firms. This chapter concludes by providing a rudimentary model for the governance of RPA based on this study.

Chapter 3 gives an overview of the research methodology used to complete the study. This chapter outlines the precise research approach, the population of the study and how a sample was selected. This chapter discussed the data collection instrument and the tools used to analyse the data.

Chapter 4 presents the study's findings discussed per the research objective developed in Chapter 1.

Chapter 5 provides analyses of the findings based on the research questions defined in Chapter 1. This chapter also develops the expanded model for RPA governance by South African firms.

Chapter 6's objective is to reach conclusions for the study by answering the research questions to determine how corporate governance should be adapted to accommodate the use of RPA by South African firms. This chapter concludes by providing suggestions for future researchers.

Chapter 2: Literature overview on the governance of RPA

2.1 Chapter introduction

This section is an empirical study of the current body of literature. This literature review will explore what academics and researchers have found on the adoption of RPA by firms with a specific focus on the elements encompassing IT governance and risk management, cybersecurity and data protection and the ethics surrounding the use of RPA by firms.

2.2 Key elements of the study

The literature review determines what the current body of literature contains on IT governance and risk management, cybersecurity and data protection, and the ethical digitalisation of firms when adopting and deploying RPA.

2.3 IT governance and risk management

2.3.1 The role of the board in ITG

According to Bergeron et al. (2015), ITG is an integral part of corporate governance, and it forms part of the duties of top management to form decision rights and an accountability framework for all individuals within the firm. The goal is to encourage set desirable behaviour from individuals and form an accountability framework for using the IT infrastructure (Bergeron et al., 2015). Asatiani et al., (2019) describe ITG as a specified decision right and an accountability framework used to encourage the desired behaviour in deploying and using a firm's IT resources. Zhen et al. (2021) add to this by stating that ITG should be used to ensure that IT-related activities align with the overall business strategy and objectives. Debreceny (2013) further suggest that organisations use ITG to ensure that the investment in IT aids in achieving the long-term and short-term strategy of the firm.

According to Hardy (2006), the role of the board in ensuring ITG revolves around (i) ensuring that IT strategy aligns with the overall strategy and goals of the business, (ii) ensuring that there are adequate structures in place to support said strategies and goals, (iii) ensuring that the firm adopts and enforces a well recognised IT control framework (COBIT and ISO 38500), (iv) marketing the IT strategy and goals

throughout the organisation and its processes, (v) providing clear, supportive and strong messages about the relevance and importance of ITG, and (vi) using metrics to measure and monitor the performance of the IT infrastructure.

2.3.2 ITG structures

Research shows that, with adequate ITG, organisations can show an average return on IT investment by 40% (Pereira & da Silva, 2012). The study also reveals that firms with well-established ITG can show increased profits of 20% compared to their competitors with the same business strategies (Pereira & da Silva, 2012; Smits & van Hillegersberg, 2018).

Three types of ITG structures are currently in use: centralised, decentralised and combined (federated) ITG structure (Asatiani et al., 2019). Centralised ITG involves a top-down approach where decision-making only happens at the top of the business hierarchy, while decentralised ITG depends on business units to make their own business decisions (Asatiani et al., 2019; Wu et al., 2015). The federated governance structure depends on centralised and decentralised governance structures (Asatiani et al., 2019). Based on the Asatiani et al., (2019) study, it is clear that the federated governance structure is the preferred structure to be implemented by firms as it is created from both the centralised and decentralised governance structures. The federated governance structure can bring autonomy and synergy to any organisation (Asatiani et al., 2019; Wu et al., 2015). However, if it is implemented incorrectly, it can result in higher barriers to IT alignment within the organisation, wasted resources and a loss in the economies of scale of deployment (Asatiani et al., 2019).

COBIT (or Control Objectives for Information and Related Technology) helps bridge the gap between business risks, value creation, control needs and technical issues (Hardy, 2006). The code is also designed to help boards implement ITG in a well-controlled manner and environment by grouping ITG objectives into four main phases: planning, acquiring and implementation, delivering and supporting and finally evaluating and monitoring (Hardy, 2006).

2.3.3 ITG risks and challenges

In recent years, ITG investment has been a significant proportion of capital expenditure by firms (Debreceny, 2013). According to Pereira and da Silva (2012), the decisions facing corporates surrounding IT adoption, management and implementation are vastly complex (Smits & van Hillegersberg, 2018), resulting in businesses losing money on bad IT acquisition. IT in an organisation creates risk by exposing firms to external threats in hacks and mitigates risk by supporting internal controls and processes (Debreceny, 2013). Debreceny (2013) thus, highlights the importance of IT and its impact on an organisation's overall risk management strategy.

The risk management strategy of an organisation is a continuous cycle that involves two main frameworks: risk analysis and risk management (van Bon et al., 2007). Identifying the risks, identifying the probable risk owners, evaluating the risks, setting an acceptable level of risk appetite/tolerance, and identifying suitable responses to risk management form part of the risk analysis framework (van Bon et al., 2007). The risk management framework, on the other hand, consists of implementing responses, gaining assurances about responses' effectiveness, and finally embedding and reviewing the responses continuously (van Bon et al., 2007).

Hardy (2006) found that ITG should have five focus areas to mitigate these IT risks. Based on the IT-related risks facing organisations, the focus areas are (and are all driven by stakeholder value): performance measurement, strategic alignment, risk management, value delivery and resource management (Hardy, 2006). These focus areas are explained in further detail in Table 1 below.

Table 1: Key facets boards should consider ensuring ITG

Focus Area	Board Considerations
Performance Measurement	Regular performance measurement using a balanced IT scorecard can be used as a tool for both the board and management to achieve organisational alignment. Using the IT scorecard, boards can address operational excellence, user orientation, and enterprise contribution.
Strategic Alignment	Boards need to ensure that the IT strategy is in line with the overall strategic objectives of the firm; ensure that IT deliverables are within budget, on time, has the appropriate functionality and benefits; direct the business resources to new markets; improve overall customer satisfaction; ensure customer retention; drive competitive strategies and distribute IT resources in such a way that it helps the business grow and reach new markets.
Risk Management	Boards need to ascertain that there is transparency surrounding the significance of the firm's risks, and they need to clarify the risk-avoidance and risk-taking policies. The risk management policies are driven by good governance to shareholders, customers, employees, vendors, and regulators.
Value Delivery	Boards need to ensure that IT delivers value by using infrastructures that enable the firm to grow and reach new markets, increase business profits, drive sustainable competitive advantage, increase customer retention, and improve overall customer satisfaction. All of which add to the value of the business model.
Resource Management	Boards need to ensure that adequate skills exist, that the appropriate methods are used within the firm to manage IT projects and that the benefits of the projects are tangible, measurable and achievable.

Source: *Adapted from Hardy (2006)*

2.3.4 ITG theories

Bergeron et al. (2015) find that many theories of corporate governance are applied to ITG across industries. The most applied ITG theories include the stewardship theory, power perspective, agency theory, resource dependency theory, stakeholder theory and the institutional theory, with the agency theory being the most widely used in practice (Bergeron et al., 2015). Research by Buckby (2011) finds that of the theories listed above, only three theories are applied in practice regularly: agency theory, stewardship theory and resource dependency theory. For this paper, we will discuss the three theories used most often in practice.

Jensen and Meckling (1976) describe the agency theory as *"a contract under which one or more persons (the principal(s)) engage another person (the agent) to perform some service on their behalf which involves some decision-making authority to the agent".* Central to the theory exists the assumption that both principals and agents are utility maximisers which means that each will not act in the best interest of the other (Buckby, 2011). This misalignment of objectives generally occurs due to the principal's problems and the conscious and unconscious self-interest of the agent (Bergeron et al., 2015; Buckby, 2011). In firms where the agency theory is evident, Buckby (2011) finds that ITG focuses on the following elements: (i) monitoring the self-regarding behaviour of IT management; (ii) the board should aim to ensure that IT management takes enough risks so that the IT risk aligns with the overarching risk profile of the firm (i.e. align the risk profiles of the agents and the principals); (iii) ensure that the board has adequate information on the role of IT governance so that agents understand what principals require regarding the IT governance of the firm.

While the agency theory focuses on the negative relationship between agents and principals, the stewardship theory assumes that the managers of a firm and the owners have a positive relationship (Buckby, 2011). Davis et al. (1997) describe stewardship theory as pro-organisational and collectivistic behaviour where this behaviour results in a higher utility than the idealistic and self-serving behaviour of agency theory. The behaviour of the stewards is collective since they seek to attain the same strategic objectives of the firm (Davis et al., 1997). Where the stewardship theory is evident in a firm, Buckby (2011) finds that the board empowers the management team rather than try and control them, and since the managers act as stewards, no close monitoring by the board is required. The study further finds that the board's role under this theory is to advise and support management with a strong relationship between the members (Buckby, 2011). ITG, using the stewardship theory, will result in management taking more risks in the IT-decision making process like supporting new technologies and having a more innovative IT infrastructure (Buckby, 2011). Unlike the agency theory, this theory supports the notion that management knows what is required for ITG as the owners of the firm can set clear goals and objectives (Buckby, 2011).

The resource dependency theory suggests that any firm's survival depends on its ability to attain and maintain resources (Buckby, 2011). The leading problem firms face is that they are not always in control of their access to recourses, and this is addressed by the theory stating that the board of directors are an essential link between an organisation and its resources (Buckby, 2011). Buckby (2011) finds that two fundamental mechanisms arise from the resource dependency theory (i) board members need to provide advice to management and counsel them to minimize the dependency of the firm on external resources, and (ii) board members outside of the firm provide preferential access to the external resources and knowledge.

2.3.5 RPA's impact on ITG and risk management

With the use of the federated IT infrastructure, RPA can be implemented in an organisation without the actual involvement of the IT department (Asatiani et al., 2019). Asatiani et al. (2019) identify this as one of the main risks facing modern firms as these technologies expose firms to security and legal issues. A study conducted by Kovanen (2020) found five main challenges when firms deploy RPA or intelligent automation. These challenges include technology risk, design and implementation risks, cyber-risks, risks related to the strategy and people-related risks (Kirchmer, 2017; Kovanen, 2020). The Kovanen (2020) study classifies technology risk as algorithm bias, data errors (incorrect data sets) and incorrect implementation. According to Kirchmer (2017), RPA risks often stem from the execution process since there is no human intervention before the program executes tasks based on specific triggers. This can result in ordering large quantities of incorrect parts or raw materials. While it is difficult to classify the risks into direct categories, since the programs are written and implemented by humans, all risks essentially stem from people and design (Kovanen, 2020).

2.3.6 Analytical perspective

From the research, it is evident that RPA poses significant risks to ITG and how the current ITG structure needs to be adapted to facilitate the use of RPA. Research also indicates that using RPA stem from the developers' biases and are not inherent in the program execution.

2.4 Cybersecurity and data protection

2.4.1 The role of the board in ensuring cybersecurity

According to Eugen and Petrut (2018), cybersecurity is the collection of tools, actions, training, risk management, assurance, security concepts, and technologies used to protect a firm's cyber environment. Rajan et al. (2021) add to this by stating that cybersecurity is used to help firms protect information integrity, confidentiality, and the availability of information by introducing managerial, administrative, and legal controls. Cybersecurity further also strives to protect a firm and its cyber network against cyber threats (Eugen & Petrut, 2018). Gartner (2021) found that IT governance, data governance and cyber vulnerabilities are the top threats facing firms in 2021 and present the most significant challenges to the board of directors.

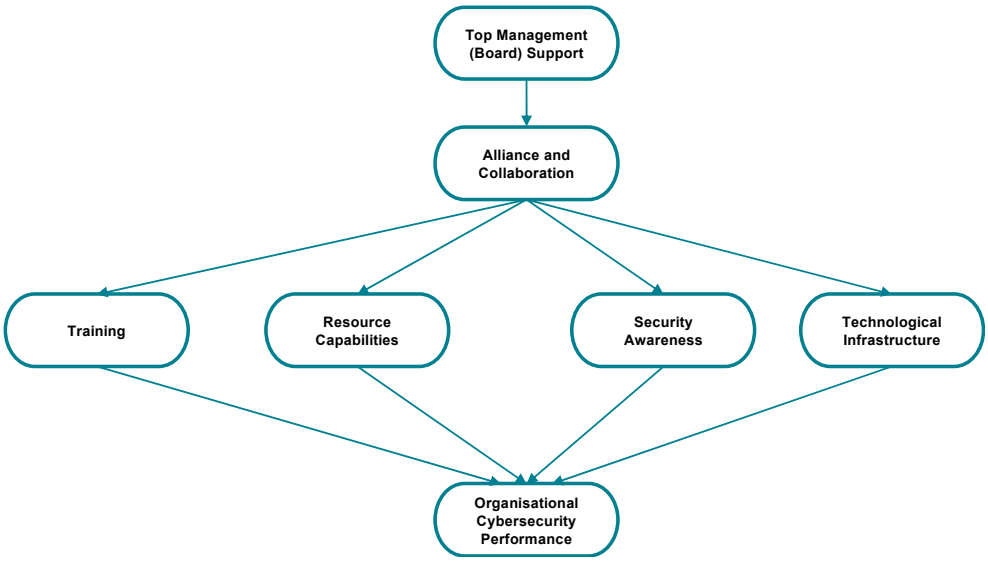
Information and the systems that house this information and business processes are an integral part of determining the success of modern firms (von Solms & von Solms, 2006). von Solms and von Solms (2006) also state that one of the most valuable assets for a firm is information. The board of directors is, thus, ultimately responsible for ensuring the protection of the firm's information assets and the remaining physical and non-physical assets. According to Rajan et al. (2021), the involvement of the board of directors and top management in cybersecurity management can result in better utilisation of company resources (IT and human) and a better formulation of a governance framework which are both vital elements to the success of the cybersecurity strategy. Hartmann and Carmenate (2021) research found that boards with IT executives are associated with a lower probability of security breaches. The study also finds a positive relationship between an IT executive, CIO or Chief Security Officer and the firm being prepared to respond to security breaches (Hartmann & Carmenate, 2021).

2.4.1.1 Cybersecurity governance

The modified total interpretive structural model (M-TISM) for strategic cybersecurity management developed by Rajan et al. (2021) proves that adequate governance increases security awareness within firms. The study found five determinants impacted by governance and cybersecurity: alliance and collaboration, resources and capabilities, training, technological infrastructure and security awareness (Rajan et al.,

2021). In figure 1, Rajan et al. (2021) graphically demonstrate how support from the board of directors can directly impact cybersecurity performance in a firm. The study found that cybersecurity management can be enhanced by good governance supported by the board of directors, and it is the responsibility of top management to set rules and regulations that can improve cybersecurity management within a firm (Rajan et al., 2021).

Figure 1: M-TISM model for cybersecurity management



Source: *Adapted from Rajan et al., 2021*

Figure 1 illustrates that support from the board of directors (top management) has a strong positive relationship with strategic alliances within a firm (Rajan et al., 2021). Strong alliances and collaborations within firms positively impact skills development and training, the development and allocation of the company's resources and capabilities, overall security awareness, and the development and deployment of the technological infrastructure of a firm (Rajan et al., 2021). Finally, Rajan et al. (2021) conclude the model by illustrating how the four elements that are impacted by top management support and good alliances and collaboration positively affect organisational cybersecurity management's performance.

From the model, the following conclusions can be drawn:

- Collaboration between the various departments within a firm can enhance cybersecurity by building and developing cybersecurity techniques, increasing awareness, and motivating employees to follow the rules and regulations.
- An increase in intercompany collaboration will result in an increased flow of information between employees, which increases the cybersecurity awareness in a firm.
- Top management's cybersecurity strategy should focus on sharing knowledge and experience with employees, which will result in increased cybersecurity awareness.
- The resources that are related to cybersecurity, such as IT infrastructure and employee skills, can be used by top management to integrate cybersecurity planning within a firm better.

2.4.2 Data protection governance

With cybersecurity comes the element of a right to privacy which can be described as a moral concept that a person has the right to make their own decisions to be let alone or not (Formosa et al., 2021). This is derived from a principle of self-ownership and the right to grant access to oneself (or a firm) as desired, as well as the right to prevent unauthorised access to private facts of oneself (or a firm) (Formosa et al., 2021). According to van Bon et al. (2007), the governance of data protection is made up of the following four elements:

- **Management of data sources:** The data sources of a firm need to be clear and well defined, while the responsibilities need to be entrusted to the right person or group of people. This process is better described as data administration and includes responsibilities like:
    - Defining the need for information,
    - Data inventory criteria and a data model must be developed,
    - Identifying data shortages and ambiguities,
    - Maintaining a data catalogue and
    - Assessing the costs and benefits of the organisation of the data.

- **Management of data standards and policies:** The board's responsibility is to formulate standards and policies for data management as part of the IT strategy.
- **Management of information processes:** All data lifecycle elements need to be controlled. The elements of the data lifecycle include accessing, collecting, creating, modifying, deleting, storing, and archiving data.
- **Management of data and IT:** This relates to the management of IT and includes the management and design of databases.

Later in this chapter, there will be further discussion on the ethical considerations of data protection, ensuring users' privacy, and protecting their rights as human beings.

2.4.3 Data protection in South Africa

de Bruyn (2014) states that data privacy laws, like POPIA, can only be effective if they include a wide-ranging set of data privacy ideologies that align to international codes like the Organisation for Economic Co-operation and Development (OECD) guidelines. These laws need to have an obligatory legal enforcement mechanism (de Bruyn, 2014). It is also essential for countries to have a data protection agency or authority that can ensure the enforcement of the laws, investigate complaints, and amend and improve the data privacy legislation (de Bruyn, 2014).

The POPI Act (POPIA) conditions impact all responsible parties that aim to collect, process or store personal information as part of the daily business activities (de Bruyn, 2014). The act defines a responsible party as *"a public or private body or any other person which alone, or in conjunction with others, determines the purpose of and means for processing personal information"* (POPI, 2013). Data protection considerations for South African firms encompass protecting individuals' data, personal information, and the firms' data. Personal data protection is governed by POPIA that came into effect on 01 July 2020 (POPI, 2013). The act entails that all firms process personal information lawfully and reasonably to ensure that no data subject's privacy rights are infringed upon (POPI, 2013). Personal information is described as any information that can identify the data subject, whether a natural person or juristic entity (POPI, 2013). Furthermore, section one of the act includes "online identifiers" as personal information (POPI, 2013), meaning that any software

tools used to enable firms to construct behavioural marketing based on an online profile created for customers are also addressed by the conditions outlined in the act (de Bruyn, 2014). Condition four of POPIA states that the processing of personal information should be done in line with the initially intended purpose of gathering the information (POPI, 2013). This is supported by the conditions set forth under the seventh condition of the act. Any person processing personal information should do so with confidentiality, and this information should not be disclosed (POPI, 2013). A study by de Bruyn (2014) summarises nine core principles that need to be present in the data protection legislation in South Africa for it to be effective. In table 2 below, we can see how these principles tie up with the conditions outlined in POPIA.

Table 2: Comparison of data privacy principles and POPIA

Principle	POPIA
Accountability	*Condition 1:* It is the obligation and responsibility of the data collector to adhere to all conditions of acts put in place by the regulatory bodies.
Collection	*Condition 2:* The collection of private data may only be done fairly, with the consent and knowledge of the subject and in a lawful manner.
Purpose specification	*Condition 3:* The collection of data can only be collected for specified use, and the purpose must be specified to the subject at the time of collection.
Purpose and rights notification	*Condition 3:* Subjects must be notified that the data is collected and for what purpose it is collected.
Uses	*Condition 4:* The personal data collected can only be used for the purpose that it was initially collected, i.e., unwarranted processing of the data is not allowed.
Data quality	*Condition 5:* The data collected must be relevant and accurate.
Reasonable security safeguards	*Condition 7:* Technological and procedural processes and practices need to be in place to ensure the safety of the personal data collected.
Data export restrictions	*Chapter 9, Section 72:* Data transfer to any other country may only be done if the intended country has acceptable data privacy legislation in place.

Source: Adapted from de Bruyn (2014) and POPI (2013)

2.4.4 RPA's impact on cybersecurity and data protection

Kovanen (2020) found that cybersecurity is built on human processes, activities, organisational processes, and information technology. If cybersecurity is not executed correctly at the start of the RPA process, it can cause severe damage and cause unintended consequences to the information technology infrastructure and data structures (Kovanen, 2020).

2.4.5 Analytical perspective

The conditions outlined in the POPIA should be considered and adhered to when South African firms deploy RPA. The act requires personal information to be processed by firms only upon receiving consent to do so. The concern for compliance with the act when RPA is used to process information is yet to be addressed and determined. No detailed research has been found on how firms in South Africa choose to protect business information when RPA is deployed.

2.5 Digital ethics

2.5.1 What does digital ethics entail?

CDR entails consumer data protection laws and privacy regulation and analysing current privacy policies, fair data practices and transparency (Lobschat et al., 2021). Formalising ethical reasoning that supports computer-enabled ethical decision making and proposing models that support responsible digital innovation also form a critical part of CDR (Lobschat et al., 2021). CDR is, thus, a new way firms can gain global competitiveness as it drives firms to strategise flexibility to adapt more quickly to the everchanging digital environment (Orbik & Zozuľaková, 2019). According to Orbik and Zozuľaková (2019), firms that actively practice CDR better understand digital trends in the market and recognise strategic digital direction faster than their competitors. These firms foster a digital culture by developing staff's digital skills and introducing new technologies to business processes (Orbik & Zozuľaková, 2019).

2.5.2 Cybersecurity ethics

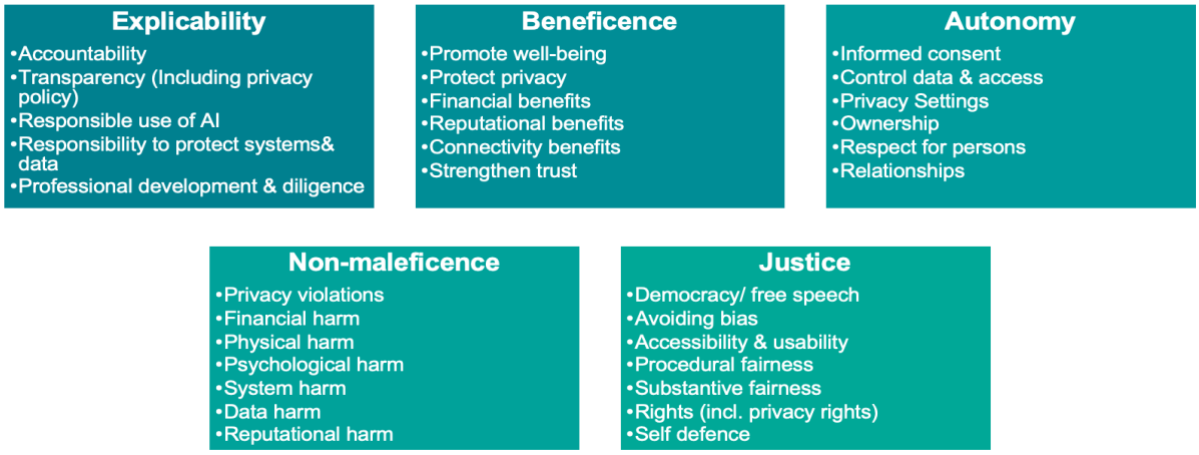
When new technologies are deployed, the ethical considerations are not limited to CDR; they also include elements of cybersecurity. Formosa et al. (2021) find that a

principlist approach to cybersecurity management yields better results than theory-driven decision making. The study explains that relying on a single general moral theory limits the board of directors given the extent of the impact cybersecurity breaches have on firms globally, and it adds that the principlist approach is more widely used in applied ethics (Formosa et al., 2021). According to Formosa et al. (2021), cybersecurity ethics should consist of the following principles:

- **Non-Maleficence** means that cybersecurity should not be used to make people's lives more complex, and it should not intentionally cause harm to the users.
- **Autonomy** describes cybersecurity measures that are used in manners that respect human autonomy, and the users have the freedom of choice around the use of the technology in their lives.
- **Beneficence** means that cybersecurity should be used to promote human well-being, and it should benefit the people who are directly impacted by the technology.
- **Justice** describes the fairness, equality, and impartiality that cybersecurity should promote.
- **Explicability** means that cybersecurity technologies are used in transparent, intelligible, and comprehensible ways as well as it should be clear who is ultimately accountable and responsible for the use of the technologies.

Figure 2 below is a graphical representation of the cybersecurity ethics principles and the elements that impact each principal.

Figure 2: Five cybersecurity ethics principles



Source: Adapted from Formosa et al., 2021

What is important to note in this model is that instead of having the sixth element of privacy, which is vital to the ethics of cybersecurity, Formosa et al. (2021) suggest that each of the five elements has its role in ensuring the privacy of data and content of the firm and its users. We can see that various privacy elements are addressed in this model, including the potential for privacy violations, privacy rights, protecting privacy, privacy autonomy, and relevant privacy policies within firms.

2.5.3 RPA's impact on digital ethics

Based on a study conducted by Kovanen (2020), digital ethics has two sides, one where RPA, as part of the digital ethics framework, behaves in an ethically questionable manner. These programs often behave in ethically questionable manners, called algorithm bias, where the programmer's bias is evident in (i) the finding of the program or (ii) training data bias where the training data has inherent discriminations and discrepancies (Beerbaum, 2020; Kovanen, 2020). The second ethical side is that some business opportunities are not followed due to the lack of understanding of the ethicality of the RPA or the RPA ethicality is too challenging to ensure (Kovanen, 2020). Beerbaum (2020) add to this by identifying various ethical considerations when firms implement RPA. Beerbaum (2020) states that RPA systems need to be transparent and accessible to ascertain the cause of actions. Furthermore, RPA processes should be auditable when decision-making is involved (Beerbaum, 2020). Both designers and builders of the RPA process should be

recognised as stakeholders in the moral implication of the use and misuse of the programs (Beerbaum, 2020). Ultimately, the programs need to be designed to be compatible with the ideals of humans and their rights, freedom and dignity (Beerbaum, 2020).

2.5.4 Analytical perspective

Studies have shown that the ethics surrounding the use of RPA is not yet well understood. There are still areas surrounding RPA and the CDR that accompanies it that need to be studied. From the current literature, it is evident that ethical considerations need to be focused on the designers of the programs more so than on the tasks that the program performs. The tasks performed should be subject to the same ethical considerations as they would have been if a human performed the tasks.

2.6 Summation of current literature on RPA governance

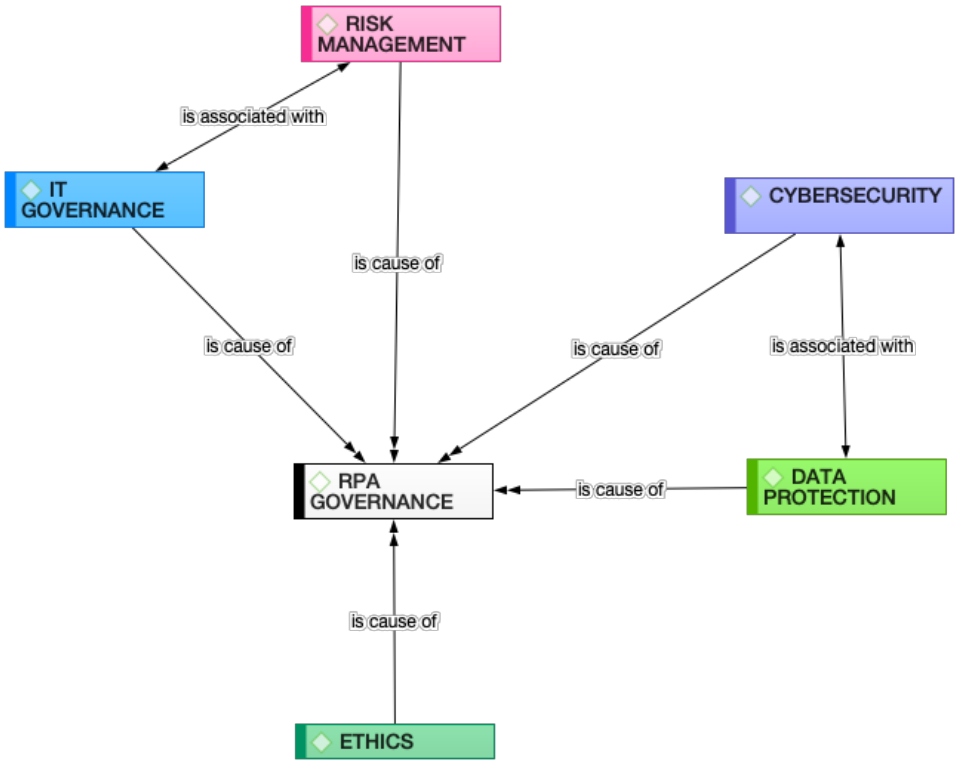
The review conducted in this section highlights the importance of governance policies and procedures when technology is introduced to a firm. In RPA adoption, ITG can be severely impacted when there are no policies and procedures to control the use and implementation of this technology. It can result in risks stemming from inappropriate use of the technology that exposes the firm's vulnerabilities. Furthermore, the adoption of RPA without the appropriate controls can lead to increased cybersecurity risks. This is due to the programs accessing and processing sensitive information. If the program and the program's implementation is not secure, the firm can face data breaches and even data losses that contravene the POPIA legislation. Finally, if a firm does not address the ethical challenges that stem from the adoption of RPA, risks surrounding the use of the program can be overlooked with dire consequences. The CDR of a firm entails that it documents adequate policies and procedures to address the digitalisation process and the increasingly digital workforce. From this, an analytical framework emerges, illustrated in Figure 3 in the following section.

2.7 Rudimentary model for the governance of RPA by South African firms

From the diagram below, we can see how ITG, risk management, cybersecurity, data protection and ethics relate to the governance of RPA. Figure 3 below is the analytical

framework formed by coding this literature section using Atlas.ti(8) and is referred to as a rudimentary model for RPA governance by South African firms. This model forms the basis of the findings of the study.

Figure 3: A rudimentary model for RPA governance by South African firms



This figure illustrates that RPA governance depends on all the elements of this study. Based on the current literature this figure shows that RPA governance is dependent on ITG, risk management, cybersecurity, data protection and ethics. This figure also indicates that ITG and risk management is associated with one another and cybersecurity and data protection are related to one another as well.

Chapter 3: Using constructivism to develop a model for the governance of RPA

3.1 Chapter introduction

This chapter represents an overview of the methodology followed to gather and analyse data for this study. The chapter outlines the research approach and design, data collection methods, population, and sampling techniques, and the research instruments. The chapter discusses the data analysis and interpretation and concludes with study limitations and ethical considerations.

3.2 Research approach

To address the specific research questions, a qualitative study was conducted. This study is an interpretive study on how the implementation of RPA impacts ITG and risk management, how cybersecurity and data protection is affected using RPA and how firms can ethically manage the digitalisation of business processes. The opinions of industry experts best answers these questions.

3.3 Research design

This study is a constructivist study based on the opinions and experiences of industry experts surrounding the overall purpose of this paper. Creswell (2013) writes that, in a constructivist study, data is collected from the researcher's view by learning from individuals' experiences and situations. Data collected in these studies are often from one or more in-depth interviews with the selected participant's (Creswell, 2013).

An interpretivism approach was used to examine and understand the viewpoints and experiences of the participants. This approach is a representational collection of data using interviews and observations (Dudovskiy, 2018). Due to the nature of the study, an interpretive approach best resulted in in-depth insights gained from participants on the research questions. Past studies on ethics, leadership and management that apply an interpretive approach are associated with a high level of validity of the primary data collected (Dudovskiy, 2018). By conducting interviews, an interpretivism approach provides understanding specific to the use of RPA and how it affects corporate governance for South African firms. According to Dudovskiy (2018), this approach also

highlights how the participants think about their problems when implementing RPA and how they deal with it.

3.4 Data collection methods

Semi-structured interviews were conducted with industry experts to understand the effect that RPA has on corporate governance. The aim was to explore the best policies and procedures for corporates actively using this tool. Interviews were best suited for this study as they helped gain a better understanding through exploring the participants' experiences, behaviours, and opinions regarding the use of RPA. The drawback of conducting interviews is that data saturation is expected to be anywhere between 10 and 15 interviews which means that the sample is limited. Data saturation for this study was reached after 12 interviews. This study aims to understand how participants develop policies and procedures when implementing RPA, which means that the limited sample size does not reduce the study's validity. The primary advantage is that the interview responses were based explicitly on experiences related to the research objectives.

3.5 Population and sample

For this study, the population consists of all firms operating within South Africa that implement, use, develop or distribute RPA. This can include firms from the financial, banking, manufacturing, insurance, mining, and retail sectors. As this is a qualitative study, a population sample was selected to conduct interviews. The sampling technique used in the study is purposive sampling where the participants were purposefully selected based on their individual experience on using RPA (Creswell, 2013). The sample consisted of industry experts in South Africa, focusing on individuals with technology experience and adoption. Research suggests that conducting between 5 and 25 interviews for a constructivist study is needed to obtain sufficient data for the study (Creswell, 2013). This study aimed to obtain 15 interview participants with experience implementing and governing RPA in the firm in various sectors within South Africa. Ultimately, 15 interviews were conducted, and one was disregarded as the information from the participant did not relate to the objectives of this study. Table 3 below provides detail on the participants of the study.

Table 3: Participant profiles

Participant	Industry of South Africa	Position held within firm
1	Financial Services	Chief Technology Officer
2	Retail	Chief Financial Officer
3	Manufacturing	Financial Director
4	Investment Holdings	Chief Financial Officer
5	Manufacturing	Chief Financial Officer
6	Financial Services	Finance Manager: ACMA, CGMA
7	Financial Services	Chief Executive Officer and Head of Automation
8	Software Developer	Senior Manager
9	Software Developer	Chief Technology Officer
10	Retail and Financial Services	Chief Operating Officer
11	Mining	Chief Financial Officer
12	Retail	Head of Business Process Automation
13	Banking	RPA Manager
14	Banking	Head of Robotics Process Automation

3.6 Research instrument

According to Creswell (2013), participants need to be asked two broad, open-ended questions covering the main sections of the research. These questions typically ask (i) what have the participants experienced and (ii) what situations or often contexts have influenced experiences of this in the past (Creswell, 2013). An interview guide using the research conducted by Creswell was created. This contained the interview questions stemming from the two categories used to perform the interviews. The questions were semi-structured to grant the subjects more opportunity to express themselves and their experiences. Focusing on the two categories of question types ensures that the data gathered is textual and a structural description of the participants' experiences (Creswell, 2013). Ultimately, the data lead to an understanding of the collective and combined experiences of the research participants (Creswell, 2013).

3.7 Procedure for data collection

Specific individuals were approached with operational experience in adopting RPA by the firm. These individuals were approached via email, telephone calls and referrals from other contacts within the firms. The data was collected by conducting individual online interviews using the interview guide and recording the interview sessions. The laws set forth by POPIA were adhered to when collecting, processing, and storing the participants' data.

3.8 Data analysis and interpretation

Data analysis is about organising data and developing themes using a set coding structure (Creswell, 2013). Once the codes are developed, the data must be presented in figures, tables or discussion (Creswell, 2013). A qualitative data analysis tool, Atlas.ti, was used to conduct a narrative analysis based on the interviews conducted. The data analysis process involved transcribing the interviews then using ATLAS.ti(8) to process the data further, which determined the relevant themes and experiences for further interpretation. Creswell (2013) describes the steps that need to be followed when analysing data collected for a constructivist:

1. Read through the written transcripts multiple times to obtain an overarching meaning for the interviews.
2. Identify any significant sentences and phrases that pertain directly to the participants' experiences.
3. Formulate meanings from the transcripts and cluster the common purposes into common themes across all participants' experiences.
4. Integrating the themes into an in-depth discussion and description of the topic studied.
5. Validating the study and the findings and including remarks from participants in the final description.

Using ATLAS.ti Creswell (2013) proposes that a coding structure would be relevant in a constructivist grounded theory study where interviews are conducted. Based on the process developed by Creswell (2013), the interviews were transcribed, read through and then using Atlas.ti(8), essential sentences and phrases were highlighted as quotations. Keeping in mind the study's objectives (i.e., the governance of RPA for South African firms in ITG and risk management, cybersecurity and data protection and digital ethics), codes were assigned to each of the quotations across the interviews.

Of the 14 interviews transcribed and coded, 1166 quotations, which contained 294 unique codes, emerged. The data were initially grouped into sub-categories that better fit the direct objectives of the study. The sub-categories (20 in total) allowed for narrowing the codes into sections that allow for better data analysis. The sub-categories were further grouped into five main categories: (i) IT governance, (ii) risk management, (iii) cybersecurity, (iv) data protection, and (v) ethics. These groups relate directly to the study's objectives, and the groupings are illustrated below. See Appendix A for the list of codes and groupings.

On Atlas.ti(8), the sub-categories were assigned to each main category by using the prefix of the prominent category name since some elements belonged to separate main categories depending on the context of the discussion. Using this defining method, a total of 32 final codes were recorded. As an example, the below quote relates to one of the benefits of RPA, which is silent recording, but it also refers directly

to the ITG category of this study where sensitive data and processes run on the computer screen:

> …in our case, as a service provider, we have got this functionality or the ability of the software to do what is called silent recording. Where it works in the background without actually physically showing on the screen or showing what it is currently processing. – Respondent A9 (2021)

The following quote also relates to the benefit of RPA as being a complement to workers and their daily tasks, but it better links to the ethics category (not replacing people in businesses) and not the ITG category as shown above:

> The response is always RPA is not meant to replace employees, but it is meant to complement them. – Respondent A9 (2021)

From this, we can see that to use just one category for the benefits of RPA is not enough and that there is evidence to support the use of the code RPA benefit under two of the main categories. Table 4 below summarises how the sub-categories relate to each of the main categories.

Table 4 visually illustrates the credibility of the research data by summarising details of the study into overlapping themes that are consistent with the scope of the research. Furthermore, the data is regarded as credible as 14 in-depth interviews were conducted with experienced respondents in various roles across a selection of industries in South Africa. The creditability of the data is also enhanced by the fact that random purposive sampling from random sectors in South Africa yielded similar evidence resulting in overlapping themes (Creswell, 2013). This means that the results and conclusion of the study, discussed in Chapter 6, are transferrable to all firms in South Africa that want to adopt or have adopted RPA.

Table 4: Sub-categories classified per main category

	IT Governance	Risk Management	Cybersecurity	Data Protection	Ethics
Access Management					
Business					
COVID					
Data Management					
Data Risk					
Data Security					
Education & Human Development					
Employment Complement					
Employment Impact					
Ethics					
Governance					
Impact on People					
People					
Process					
Risk					
RPA					
RPA Benefit					
RPA Disadvantage					
RPA Security					
Technology					

3.9 Limitations of study

- This study was limited to firms that actively used RPA in the business processes and did not consider firms that have yet to implement this technology.
- The sample was purely South African firms, but it was not limited to firms with a footprint only in South Africa, as some firms did have global branches.
- The interview guide was developed to analyse the South African operations of said firms.

3.10 Ethical considerations

An ethics clearance (number: WBS/DB1171378/417) from Wits Business School was obtained using the HREC Non-Medical clearance specifications. The ethics clearance

certificate can be found in Appendix E of this study, the participant information sheet under Appendix B and the informed consent form under Appendix C.

This study does not involve questions about participants' vulnerability and does not cause any potential risk or harm. No demographic or other personal identifying information was gathered from participants as this would not impact the study's outcome. No information was collected on the specific organisation outside of the purpose of the study. Subjects' participation in the study was voluntary, and no incentives were offered to potential interviewees. Formal, signed consent was obtained before the interviews commenced. No personal information is disclosed to other participants in the study, and participants are not identifiable in their responses during interviews. The study does not contain any restricted or confidential information that may not be in the public domain. The individual identities of the participants and firms are not identifiable in the raw data set as pseudonyms are used. All the data collected is stored on a password-protected computer, and after five years, it will be destroyed. A data set backup was made on the cloud at regular intervals, accessible by password.

To ensure the anonymity of participants, codes were assigned as pseudonyms to identify the participants. From this point forward, all participants will be referred to by their respective pseudonym codes (A1 – A14).

Chapter 4: Study results on the governance of RPA

4.1 Chapter introduction

This chapter represents a presentation of the findings of the data collected. This chapter will be discussed per the research sub-questions developed in Chapter 1 of this study:

- Findings relating to how ITG and risk management are impacted by implementing RPA.
- Findings relating to ways in which the use of RPA affects cybersecurity and data protection.
- Findings relating to how a South African firm can ethically manage the digitalisation processes when adopting RPA.

4.2 Findings relating to how ITG and risk management are affected by implementing RPA

To understand how the adoption of RPA effects ITG and risk management by South African firms, the study sought to establish how the ITG structure is affected using RPA, what governance challenges individuals in the firms faced, how risk management was affected and whether they experienced any change in the risk management strategy.

4.2.1 Effect of RPA on ITG structures

Participants were asked whether they have had any significant effect on the ITG structure of the organisation since adopting RPA. Of the 14 participants, the minority indicated that a change in the current governance structure is required to accommodate using RPA, while the majority confirmed that the existing structures are sufficient for the use of RPA.

Respondent A7 (2021) indicated that a change to the ITG structure was required only due to the decentralised nature of the current ITG structure and the legacy systems in use across the businesses within the organisation structure. In contradiction to this, the study also finds that RPA could fit into the ITG of a firm with a fragmented ITG (Respondent A12 (2021)), indicating that RPA governance could fit into any ITG

structure. The data illustrates that the current ITG structure of firms could be sufficient to accommodate the use of RPA, whether the structure is fragmented or not, but that some considerations need to be made to ensure that the software is adequately controlled and monitored. Based on the data, the elements of existing ITG structures that could accommodate the use of RPA include user access, user roles and integration like with any typical computer software program (Respondent A4 (2021) & Respondent A11 (2021)).

One of the considerations highlighted by the study is that firms need to ensure that their current ITG structure has enough controls and security protocols to accommodate the use of RPA. Even if there is no formal policy for using RPA, it should be added to the ITG policies already in place (Respondent A6 (2021)). The data supports this by showing that it is expected that some changes may be required in the future, whether it is on policy amendments or to the structure and controls itself (Respondent A5 (2021)). Respondent A4 (2021) expressly indicated this by stating that the ITG structure was sufficient for the use of RPA but that some policies had to be amended to allow RPA software to access parts of the system previously accessed by people in the firm:

> …actually had to go and change their policy to allow non-flesh and blood users to be granted access to the ERP system because their policy is restricted to only flesh and blood.

On the other hand, Respondent A14 (2021) indicated that the internal controls department was involved in advising how the ITG structure should be adapted (if needed) to accommodate RPA and the risks associated with using RPA. The assumption was that the current controls in place for human workers would be insufficient for the use of RPA:

> The robot is going to be able to access multiple systems… if somebody gains access to your robot, they actually gain access to multiple systems and platforms across the group.

The study also finds that the opposite is true in that RPA needs to be governed like any other employee of the firm based on the current ITG structure in place, as stated by Respondent A9 (2021) below:

> … the same governance that you provide to an employee in terms of what systems they can access and so on, that also applies … to the robot.

Respondent A2 (2021) advised that the focus of the RPA had been on implementing the project and not on the impact the use of the software would have on the current ITG structure of the firm.

4.2.2 ITG challenges due to RPA adoption

In this questioning section, participants were asked whether they have experienced any ITG challenges since adopting RPA. Of the respondents, nine came across various challenges, four have not encountered any ITG challenges to date, and one had no comment on this study section. Of the 9 participants that have come across some ITG challenges, some had difficulties with the people aspect of implementing RPA, some had IT challenges, and some had information challenges that correspond to the enforcement of POPIA.

Respondent A1 (2021) indicated that they faced a challenge regarding selecting the process to automate using RPA. In addition to this, they also had difficulties in implementing controls for automated processes after RPA was implemented (Respondent A1 (2021)). The study indicates that firms that do not make all of the considerations discussed in the previous sections found that initial processes need the same level of controls as new processes, and building the controls into an existing RPA process is challenging.

The study also finds that one of the main challenges respondents face is revolving the people involved with or impacted by the RPA adoption. Respondent A4 (2021) indicated that their challenge revolved around people not monitoring either the automated process or output once the RPA program is deployed to that specific process. The challenge is also that people did not necessarily understand the technology (Respondent A5 (2021)) and assumed that they would no longer need to be involved in the automated process (Respondent A4 (2021)). People not understanding RPA technology means that the framework in which RPA operates is not adjusted for the program to do so efficiently (Respondent A5 (2021)). The study finds that getting people in the business to understand what RPA is about and how

RPA would fit into the daily workings of the company is one of the critical success factors of implementing RPA.

The study finds that firms have had ITG challenges in the form of the risk of malicious intent of workers that interact directly with the software and the lack of understanding of how the programs will work and what controls need to be in place, as indicated by Respondent A11 (2021) below:

> … a lack of understanding of the technology itself and having this notion of… the bots doing a payment… and potentially do a wrong payment… and the other was can people hack the system and essentially get the bot to do payments for themselves?

The study finds that firms have had IT and information challenges since adopting RPA. Respondent A6 (2021) indicated, for instance, that the firm's ERP system had to be segregated from the rest of the business to ensure information security when the robot accessed and processed data. Another IT challenge this participant faces is ensuring that the servers are secure and have the necessary confidentiality and access control measures (Respondent A6 (2021)). In addition to access control, Respondent A7 (2021) faced a challenge where the RPA robot would require more system access than any other individual allowed to have in the firm. This gave rise to policy challenges and additional risks that were not considered when RPA was adopted by this firm, as indicated by Respondent A7 (2021) below:

> … the bot has a login like a human. And the more tasks you add to the list of the bot, the wider you almost have to open that user's profile. So, the question would come up, you know, so can this bot now do what we would not have allowed a human to do?

Furthermore, the study finds that firms face information security challenges when implementing RPA. Respondent A8 (2021) indicated that the significant challenges faced by the firm were related to information security due to the fragmented storage of client information within the organisation. In addition to this, the ITG challenges stem from the sharing of sensitive company information. When the RPA robot is running a process on a computer screen, anyone with physical access to that screen will also gain insight into the data being processed, as indicated by Respondent A9 (2021):

> … that gives a challenge in the sense that you now need this physical device to be secure so that… someone passing by does not see any sensitive information processed by the bot…

Finally, the study also finds that firms face challenges regarding the access granted to the RPA robots and the control of the passwords issued to the robots to perform the set tasks. Respondent A13 (2021) makes specific reference to access control and password security when the RPA (referred to as the firm's virtual employees) is deployed to automate tasks:

> Now one of the biggest challenges I had is that each of these virtual employees… would need to have specific passwords created so they can access those applications to execute the task at hand…

While the previous participants have faced specific governance challenges regarding information security, Respondent A2 (2021) addressed some of these by changing the organisation's policies based on the principles set forth by POPIA.

4.2.3 The effects of RPA on risk management

Participants were asked whether the adoption of RPA influenced their firm's risk management strategies or whether RPA had a specific impact on the daily risk management of the firm. The majority of the participants indicated that they had a change in the day-to-day risk management of the firm, or the risk management strategy had changed to accommodate RPA. The minority of the respondents showed no difference in risk management in the firm.

The study finds that risk management for firms is a continuous exercise and that a change in risk management is not primarily influenced by the adoption of RPA (Respondent A1 (2021) & Respondent A3 (2021)). The respondents refer to RPA assisting in managing and mitigating risks once deployed into various firms. One way RPA mitigates risk is by having robots replace human processes, the number of errors in tasks decreases significantly, and efficiencies improved (Respondent A5 (2021) & Respondent A14 (2021)). Respondent A4 (2021) indicates that since the RPA process is designed to replicate the same function multiple times that it will not make any mistakes and that it led to a reduction in risk for the firm:

> …where we have been able to deploy bots to perform those sort of management functions, or maintenance functions, backups, and … moving things around… it has actually made our lives quite a lot easier. Because once you build the process into the bot and the logic works perfectly, it is going to work perfectly every time.

The study supports this theory by finding that RPA as software is developed and designed not to do work incorrectly. The software aims to eliminate human intervention and error as it is purposely built to replicate tasks (Respondent A14 (2021)).

In addition to the above, the study finds that firms will face new risks when they adopt RPA. Up to this point, the focus has been on RPA being a tool used to mitigate the existing risks faced by firms. Respondent A14 (2021) indicated that new threats arose when the software was deployed since the robots now access multiple systems from the same point of entry and because these robots generally have more access than what would be granted to a single employee in the firm:

> … if you happen to be able to access the robot, your risk is going to be very much higher because of its ability to access multiple systems... So, you have a much higher risk exposure if you happen to hack into the robots' access as opposed to individual's access…

Respondent A8 (2021) finds that the use of RPA increased the risks faced by their firm due to the nature of the access to the programs. It is evident from the data that access management is another critical success factor when firms deploy RPA.

In addition to access management, the study finds that control failures are a significant risk encountered by the firms since adopting RPA (Respondent A10 (2021)). At the same time, the data support this by indicating that firms need to be aware of all risk factors throughout the entire cycle of an RPA process for it to be successfully implemented, as indicated by Respondent A11 (2021):

> The risk of introducing the bots into the workplace, from a risk community perspective, …is obviously making sure that in the whole life cycle, (and) the risk factors are taken care of.

The study highlights the risk of malicious intent of employees, also discussed in the previous section. Respondent A9 (2021) identifies this risk of malicious intent and

indicates that the workers directly involved with developing the RPA software within a firm pose the most significant vulnerability:

> …some people can actually manipulate them and start doing fraudulent transactions. And if this happens, then it can be difficult to trace if you do not have proper control of your RPA infrastructure.

While the study identifies the risks firms face when adopting RPA, it also highlights how firms can manage these risks. Respondent A13 (2021) advised that their firm manages RPA risk by ensuring that the RPA process alerts the responsible parties when necessary. They have RPA reports and logs that can be used to identify any problems.

4.3 Findings relating to ways in which RPA affects cybersecurity and data protection

To understand how the adoption of RPA effects cybersecurity and data protection, the study sought to establish which cybersecurity aspects needed to be considered when deploying RPA, how RPA affected data protection and data security, where the RPA software accessed and processed information and finally, by determining which challenges the firms faced when RPA was adopted.

4.3.1 Cybersecurity considerations for the adoption of RPA

In this study section, the participants were asked which cybersecurity aspects were considered when the respective firms initially adopted RPA. Initially, some firms did not consider cybersecurity aspects which means some controls were absent from the design and implementation of the software (Respondent A1 (2021), Respondent A2 (2021) & Respondent A14 (2021)). The study finds that after this initial implementation, some firms had cybersecurity considerations included as aspects of the RPA program's security and the platform's security on which the RPA program runs its tasks, as indicated by Respondent A1 (2021):

> … we need to make sure that our client data is protected and (that) we do not have a weak spot in RPA as a cyber security risk. (And) even though RPA makes it more secure, you still need your platform to be secure…

In addition to this, the study finds that some firms' existing cybersecurity protocols are sufficiently suited for the use of RPA and that no additional vulnerabilities will arise from adopting the software (Respondents A3 (2021) & Respondent A7 (2021)). Respondent A4 (2021) adds to this by indicating that software used by the firm already has adequate cybersecurity protocols installed but that they do perform regular penetration testing on the software as an additional security measure.

The data shows that general cybersecurity principles need to be applied when firms adopt RPA, similar to any other software introduced to a firm. These principles include firewalls and off-site recovery sites should there be operation risks, fires, or theft (Respondent A5 (2021)). Respondent A9 (2021) supports this by stating that the same cybersecurity measures used by firms on the current software used by the firm should be applied to the implementation of RPA as well:

> … the same security measures that they put when they are… not using RPA would be the same measures that they need when they are using RPA.

Respondent A6 (2021) is the only participant to mention a Chief Technology Officer (CTO), and cybersecurity was one of the focus points of the business when they decided to deploy RPA within the firm.

> … cybersecurity was definitely a big consideration when we started with RPA… our CTO…was more involved in that aspect to make sure that we do have the necessary processes and controls in place to make sure that no data is leaked or is accessed by anyone that does not have the proper access.

4.3.2 Data protection and data security considerations when firms use RPA

With the introduction of POPIA regulation, it is essential to discuss the protection of data and data security measures used by firms. The minority of the participants make mention of POPIA when talking about the steps taken to ensure data protection and data security in the firms. Respondent A1 (2021) confirms that the software used by the firm could not store data after processing it, thereby ensuring that data is not stored on servers for anyone to access that does not have permission to access it:

> … data protection in South Africa has now become a big thing because of POPIA. So that would mean that you need to limit your amount of personal data that you keep on

> record. (RPA has the) functionality of not keeping the data at all… limiting our exposure of personal information as well as the client's exposure…

Regarding the data protection protocols set in place when deploying RPA, the study finds that data security entails access control which needs to be applied to the whole firm, including the RPA robots. The data indicates that the existing data governance policies are sufficient for some firms to secure data when RPA is adopted (Respondent A8 (2021)). Respondent A3 (2021) expressly indicated that access control was the primary consideration for their firm and that the deliberations made included the policy around what access the RPA should be granted to perform the tasks it was designed for:

> … one of the most important aspects of data security for the use of RPA is that access control. You need to make sure that the access you provide the bot with is the access that you want it to have and that it does not have access to things and data that it has not meant to have access to.

The study also indicates that firms need to formulate or amend data protection policies to provide guidelines for using RPA within that firm. Respondent A2 (2021) suggests that firms need to ascertain whether the use of RPA will breach any of the overarching security protocols in the current policy before the software is adopted. According to Respondent A14 (2021), RPA needs to be governed similarly to employees of the firm since the robots will be used to replace the processes previously performed by the employees:

> … the robot is doing the same work as an employee would be doing, and we, therefore, have the same controls in place regarding the storage and salvage of that data in terms of the firewalls that we have.

The study finds no data security risk if a robot only processes information and does not store it. The risk arises when the processes need to access information stored outside the RPA environment. Respondent A4 (2021) indicates that should the robots access data in a firm's secure environment, the typical ITG policy should apply to keep data and the server safe. Respondent A12 (2021) supports this by stating that should the RPA process need to save data it accessed, the data would be governed within the existing policy:

> … where the bot access data, we are not saving data if we do not have to use it in another process... If we do save data, we make sure that it adheres to our general IT protocols of how we need to save things…

The study highlights one of the manners in which RPA mitigates the data security risk by indicating that the software can process data and execute tasks without needing to store the data. Respondent A9 (2021) suggested that the software program used by the firm is primarily used in a mode where data processing is not visible on a computer screen, and only the process log is accessible for monitoring. According to Respondent A9 (2021), this method of RPA deployment is selected as it offers the most security on the sensitive data that the robots process:

> …we have… the ability of the (RPA) software to do what is called silent recording. Where it works in the background without actually physically showing on the screen or showing what it is currently processing. So that gives an extra layer of security in the sense that a human being cannot intercept some of that data.

Additionally, the study finds that RPA software in South Africa has the functionality not to use the silent recording mode and instead opt for the standard processing modules of the program. In such instances, the firms use data encryption and credential vaults as cybersecurity and data protection measures (Respondent A9 (2021) & Respondent A12 (2021)):

> … there is also encryption, where the data is encrypted when it is in storage. So, for example, a lot of the RPA providers have what we call like a vault; you store any sensitive data such as username and passwords for accessing certain systems…

Furthermore, Respondent A11 (2021) indicated their firm uses encryption applied to processes that are executed by the RPA robots as an additional cybersecurity measure:

> … you can encrypt the queues that the bot actually processes on so nobody can see what is actually being processed from that perspective…

As a final cybersecurity measure, Respondent A13 (2021) indicated that their firm uses virtual environments where the RPA program accesses and processes data. One of the main features of this virtual environment is that it has restricted access and has

secure access logs for anyone that accesses the tool. This helps to reduce the risk associated with data security when RPA is used.

4.3.3 Data protection or cybersecurity challenges faced by firms

This section of questioning revolved around whether firms have encountered any data protection challenges since implementing RPA in the respective firms. The minority of respondents have encountered challenges, while the majority have not encountered any cybersecurity or data protection challenges since implementing RPA.

The study finds that one of the main challenges firms face is regarding users and segregating access to ensure they do not have the access they are not meant to have (Respondent A1 (2021)). The data also shows that user segregation and making sure that usernames and passwords are of the acceptable standard were some of the challenges faced by participants of this study (Respondent A11 (2021)). The data indicate that hosting data in the cloud presented the participants with a significant cybersecurity challenge as data security could more easily be compromised if held in the cloud (Respondent A9 (2021)).

4.4 Findings relating to how South African firms can ethically manage the digitalisation process when adopting RPA

This section of the study aimed to determine what ethical considerations need to be addressed when South African firms adopt RPA. The participants were asked whether they made any specific ethical considerations and encountered any ethical challenges. With unemployment being topical in South Africa, the participants were also asked whether they have experienced job losses or expected to come across job losses due to the implementation of RPA.

4.4.1 Ethical considerations when firms deploy RPA

In this part of the questioning, the participants were asked whether they made any ethical considerations before or during the use of RPA by the firm. The majority of participants indicated that they made specific ethical considerations, while the majority stated that they did not make special considerations due to the existing company

policy or moral culture. Some participants only discussed the impact on the employment of the firm.

The study finds that since this technology is new, careful consideration needs to be made regarding the biases of the programmers that can filter through to the coding of the robots. Other data shows that firms need to consider fairness regarding using personal data and not exploiting the information that the robot processes to benefit the firm and disadvantage the other party concerned (Respondent A5 (2021)). The biases from the study can take the form of prejudice against race, sexual orientation, or age as per Respondent A1 (2021):

> Considerations need to be made for an unbiased (RPA) process where tasks are built without any prejudice against any race, sex, or age. And that bias is not intentional; it is completely unintentional, but you will not know how a bot will react to something that comes in that is now completely different than what it used to be…

The data indicates a specific ethical dilemma a firm faces when they deploy the software in the firm. Depending on the purpose of the RPA program, it could arise that it would need to log in to some systems and retrieve or deposit data files to execute the task. Some programs like banking platforms and websites are designed with anti-bot software, preventing the robots from accessing the systems. According to Respondent A4 (2021), there are ways in which the bots can be programmed to mimic human inputs, which will allow the robot to access the system with the anti-bot software on it.

> … some websites have these anti-bot software… the ethical question is that if they are trying to keep bots off, but you can circumvent their anti-bot software, should you tell them that they might as well switch the antivirus software off?

4.4.2 The effect of RPA on the employment of firms

In this final section of questioning, the participants were asked whether they have experienced job losses or are expecting to experience job losses in the future due to RPA. The majority of the participants indicated that they had not experienced job losses and could reskill or redeploy employees, and a single participant experienced job losses.

The study finds that firms have not experienced any job losses due to the employees being redeployed to other aspects of the organisation or reskilled depending on the firm's requirements. The data shows that some firms were able to take the existing workforce and the additional capacity created by RPA, and they were able to put these employees into training and assign new tasks to them (Respondent A1 (2021) & Respondent A12 (2021)). Respondent A14 (2021) supports this by stating that RPA deployment resulted in employees being reskilled and used for functions that RPA robots cannot perform:

> … currently, in the organisation, there is no job losses due to RPA. So, what we have done is we have looked for opportunities where we could automate and in the areas where we automated… we are just reskilling the people elsewhere.

Respondent A4 (2021) indicated that their firm is growing, but instead of hiring new people, they can make the current workforce more productive by adding RPA to the processes. This ensures that RPA does not cause job loss to the firm and increases the overall efficiencies of employees. Respondent A9 (2021) states that their RPA strategy was not to replace employees but rather to complement their current function within the business:

> … RPA is not meant to replace employees, but it is meant to complement them. So, the intention is to take away the manual and repetitive tasks… so that (people) are freed up to more human-like work or value-adding work…

The study indicated that firms that did not experience any job losses due to the use of RPA had increased the employee's ability to do tasks that they were not able to do in the past (Respondent A11 (2021)). This is not a strategic reskilling of employees but rather a natural cause when employees' manual workload is reduced. Respondent A6 (2021) found that they did not need to replace people as expected when they initially deployed RPA but rather used people in conjunction with RPA to perform the work at hand:

> … deploying an RPA bot to basically perform certain functions which would then replace the need for an additional resource… it was found that the scope of the tasks and the requirements associated with it was far wider than just manual data processing. So, we would still need that resource to perform certain functions that RPA cannot do.

In addition to this, Respondent A6 (2021) also states that it is the responsibility of any organisation to reskill and redeploy people within the firm when they decide to adopt RPA:

> I feel our ethic responsibility is to ensure that in future… these roles that RPA is going to replace, we need to either educate or enable these people to still have a means of income.

The study finds that some firms could employ new skills in the firm that they would not have hired before. Respondent A2 (2021) indicated that since adopting RPA, they have eight skilled workers they would not have employed before. Some were redeployed from the department where RPA was used, and some were newly appointed.

The reality faced by firms in this study is that even though they have not had job losses to date, at some point, all firms will experience job displacement in the future. This is mainly due to:

- Firms are redeploying existing workers rather than appointing new ones.
- the employees are not upskilling and changing their abilities to perform tasks that robots cannot do

To counter these job losses, firms can aim to reskill workers, but this will likely not be a solution for all of the firm's employees (Respondent A2 (2021)):

> The intention is to upskill and train, but inevitably that is not always going to happen… (there will) definitely be a displacement with people when you introduce an RPA.… because you have got a lot of people that are just doing routine jobs that are not necessarily adding value…

The study finds that one of the benefits of using RPA is that the overall output of firms increases without increasing the workforce required for the same output volume. According to Respondent A7 (2021), employees are now making decisions and investigating problems rather than doing repetitive manual work, which RPA replaced:

> I think the benefit of RPA is to deal with increased volume without increasing people and to free up people to allow better utilisation of the human judgement of what is right

> and wrong based on a processing of a transaction or what is an anomaly, or what is outside of the ordinary…

One participant in the study experienced job losses, not due to the adoption of RPA, but RPA did enable the firm to absorb the employees' work. In this instance, Respondent A8 (2021) states that the business would have had to cut jobs due to the financial restraints on the firm at that time:

> …15 people were actually axed because of the implementation of RPA in that particular unit. That company did not really have much of a choice, though, because shareholders and management was also forced… (due to) cash flow that they really had to do this.

While the study finds that firms may not initially experience employment loss, it may be inevitable for some firms to reduce the workforce. The data shows that this impact on employment is not primarily in the control of the management of firms. It is also the responsibility of employees to ensure that they have the skills to do work that RPA robots cannot do. The study further finds that while RPA can improve efficiencies of processes and increase workers' productivity, this may also enable firms to reduce the workforce of firms.

Chapter 5: An expanded model for the governance of RPA

5.1 Chapter introduction

In this chapter, the findings from the study concerning the elements outlined in the problem statement is discussed. This discussion will be structured according to the research questions proposed in Chapter 1.

- How ITG and risk management are affected by implementing RPA.
- Ways in which the use of RPA affects cybersecurity and data protection.
- How a South African firm can ethically manage the digitalisation processes when adopting RPA

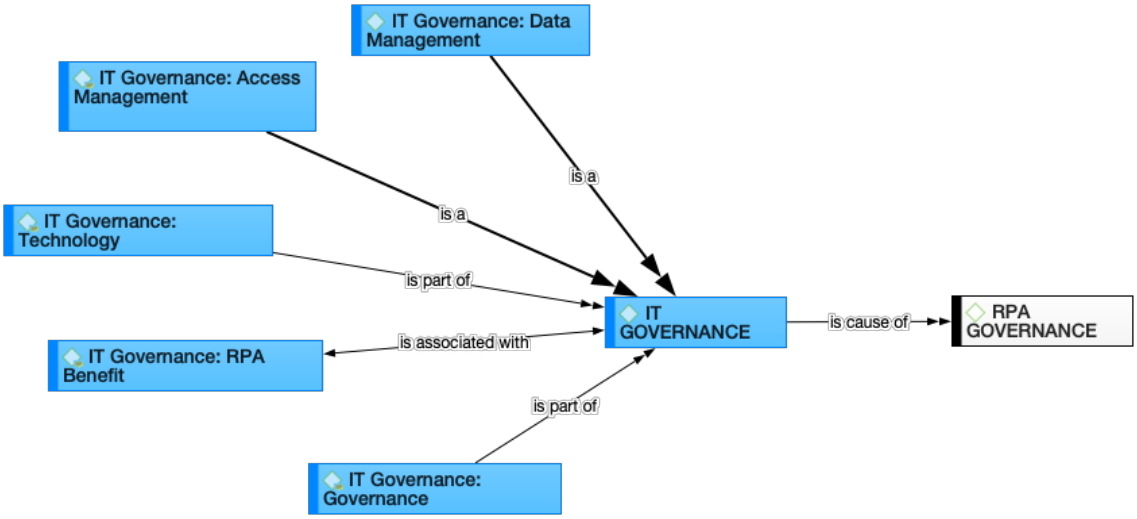
This chapter develops a model for the governance of RPA for digital business in South Africa by focussing on each individual element of the study and concludes with a single combined model of the findings from the data. The model is built by using the data from the study and some findings are supported by existing literature.

5.2 The adoption of RPA and its effect on ITG and risk management

5.2.1 The effect of RPA on ITG structures

The study focused on participants' perceptions of how their ITG structures were affected by using RPA in the firm. The study reveals that the main elements of ITG that need to be addressed by RPA governance include data management, access management, and general ITG. Furthermore, it was revealed that some of the benefits of RPA and the technology are associated with the ITG perspective of implementing RPA. These elements are graphically presented in Figure 4 below:

Figure 4: Elements of ITG concerning the governance of RPA



The study finds that data management as part of the ITG strategy deployed by firms can involve moving some servers off-site after implementing RPA. This protects the data housed in the on-site servers that the robots will not access. The RPA tool could aid in data management by ensuring that data is always protected and secure. One of the benefits of using RPA is that the robots can work in a "silent" mode where the process and information are not shown on the PC screen, thereby automatically protecting the data. Being aware of the benefits that RPA can bring to the business can be used by firms to enhance their ITG structure and policies.

Access management is the second section of ITG that impacts the RPA governance of a firm. This part of RPA governance stems from robots gaining access to systems through passcodes which creates vulnerabilities in the ITG structure of the organisation. The study finds the following elements of access management that impact the ITG of firms:

- Password control for users across the firm
- Credential vaults or a password safe for the usernames and passwords used by RPA robots to ensure no human can intervene in the RPA process

Technology and technology advances are at the centre of the deployment of RPA. Firms will need to adapt ITG structures to accommodate the changes accordingly with technology. The study finds that selecting the right RPA technology and ensuring that the security built into the platform is sufficient is one of the leading considerations firms

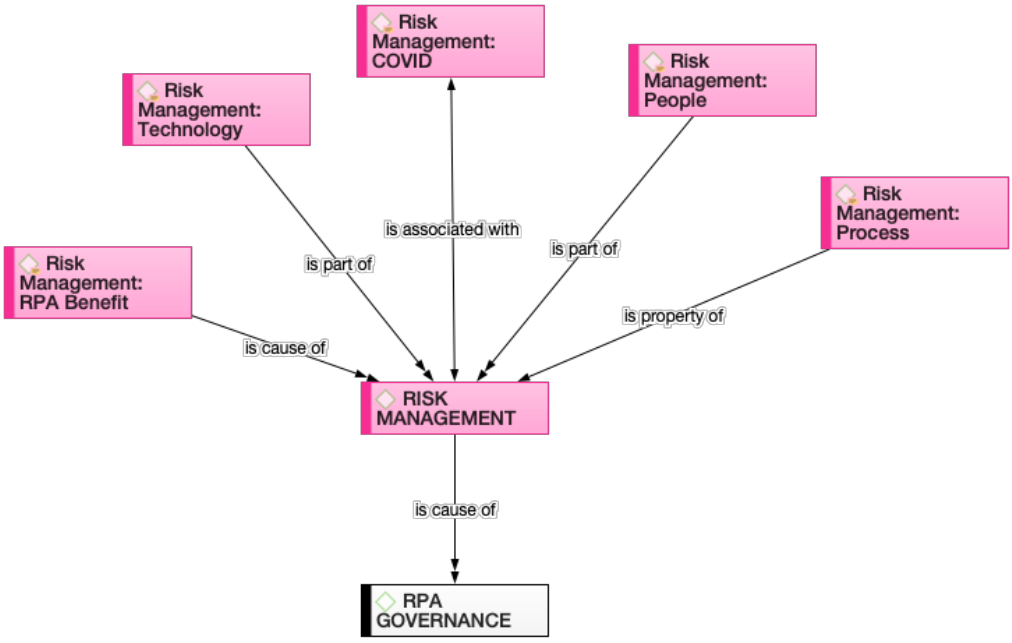
in South Africa need to make when they adopt RPA. The technology should provide firms with the ability to offer different roles and responsibilities to people who are involved in the RPA process. This is supported by what Asatiani et al. (2019) described as ITG, where ITG is an accountability framework to encourage desired behaviour from employees when they use a firm's IT resources. This means that RPA would need to fit into the firms' existing ITG framework, ensuring that the RPA governance principles align with the general ITG principles already established by firms. Zhen et al. (2021), also supports this by stating that ITG ensures that other IT—related activities (like RPA) need to align with the existing business objectives.

The data from the study finds that data management and access management are ITG management tools. At the same time, RPA technology and the benefits of using the technology are closely associated with ITG in a firm that adopts RPA. General ITG principles need to be applied when firms use RPA. All the elements (i) data management, (ii) access management, (iii) RPA technology, (iv) the benefits that stem from using RPA, and (v) general ITG form a holistic approach to ITG of a firm that adopts RPA. This also shows that ITG is a crucial element in the governance of RPA as per the purpose of this study.

5.2.2 The effect RPA has on risk management

This section of the study focused on participants' experience and a change in their risk management strategies based on the implementation of RPA. The study reveals that the main elements of risk management that need to be addressed by RPA governance include process risk, people risk, general risk considerations, COVID and technology risk. Furthermore, it was revealed that some of the benefits of RPA are associated with active risk management in South African firms, as shown in Figure 5 below:

Figure 5: Elements of risk management concerning the governance of RPA



This study finds that one of the biggest challenges firms face is selecting the processes to automate. The best processes to automate are the ones that reduce the risk to the firm, and these processes should form part of the initial adoption of RPA within firms. By automating the "broken" process, firms add complexities to the business and the RPA adoption process that does not benefit the firm. This could also result in RPA projects failing. According to Kirchmer (2017), RPA risks often stem from the execution process since there is no human intervention before the program executes tasks which is in line with the findings from the data. Kovanen (2020) also supports the data from the study by stating that all risks essentially stem from people and design when implementing RPA. Firms should aim to automate processes that run smoothly and efficiently to ensure the successful implementation of RPA.

The study highlights one of the risks that any RPA governance policy needs to address. This is the risk of malicious or fraudulent intent either by the software developers or any person who would have access to the software at any point in time. These people could create codes and instructions that could benefit them (financially or otherwise) while not detected by the controls set for the RPA programs. The data indicate that RPA programs cannot go rogue by default; only poor testing or inadequately designed processes can cause defects in the programming. The risk that RPA governance policies should address should include detection mechanisms for

deliberate sabotage and fraudulent processes or transactions. The study also highlights that improper controls could compromise the firm's data. According to van Bon et al. (2007), identifying risks, as highlighted by the data above, should be one of the first steps in the risk management framework of an organisation. Evaluating these risks and setting acceptable risk appetite levels complete the risk analysis framework (van Bon et al., 2007).

The data shows that the use of RPA did assist firms in managing risk during the COVID-19 pandemic. Having people work from home meant that their data protection and data security risk increased as people would access secure networks from unsecured local connections. The firm then deployed RPA to help get information from the secure servers and deliver it to employees in the required format by a simple prompt. Debreceny (2013) supports the data by stating that firms can use IT to mitigate technology risks by supporting internal controls and having processes (like this) in place. The study also finds that the use of RPA has reduced risk in the firms by increasing reporting accuracies and the protection of data that comes with the help of RPA.

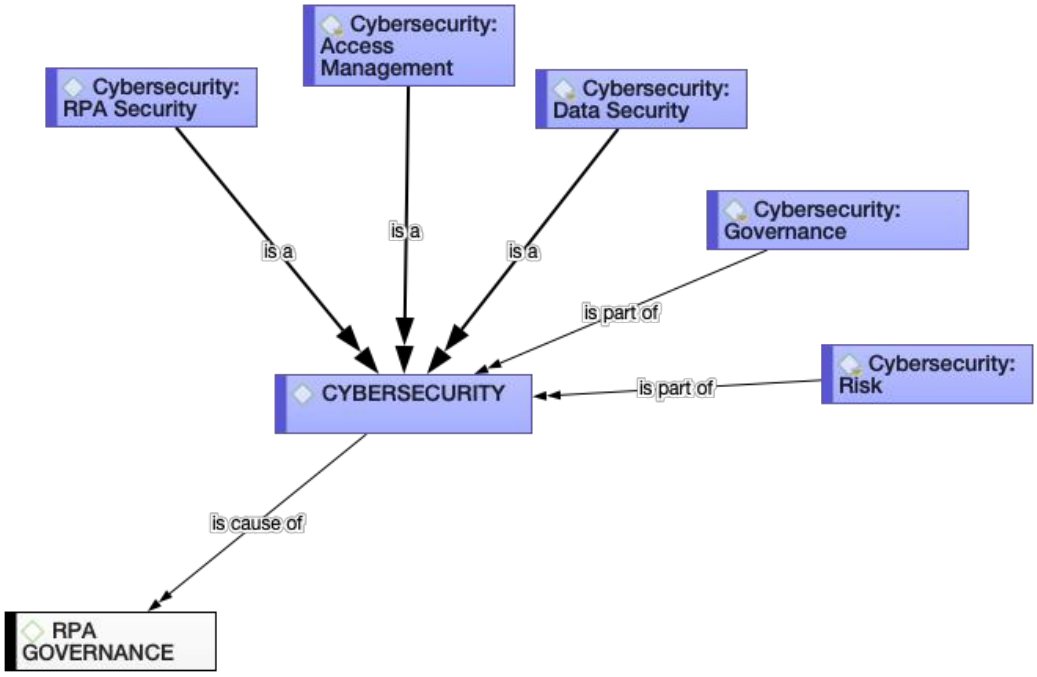
The data from the study finds that the risk management function in South African firms is a critical element that needs to be considered in the governance process of RPA. This risk management function is dependent on multiple individual components, including (i) process risk, (ii) people risk, (iii) pandemic risk, (iv) technology risk and (v) the benefits of using RPA as a means to mitigate other risks.

5.3 The adoption of RPA and its effect on affect cybersecurity and data protection

5.3.1 The effect of RPA on cybersecurity management

In this section of the study, the focus was on participants' experience with aspects of cybersecurity and the challenges they faced when implementing RPA. The study reveals that the main elements of cybersecurity need to include the security of the RPA program, protection of the firm's technology, access management, data security, general cybersecurity governance and cybersecurity risk, as illustrated in Figure 6 below.

Figure 6: Elements of cybersecurity concerning the governance of RPA



The study identified the use of RPA has potential data security and cybersecurity risk in their firm. In addition to this, the data shows that even though RPA does pose a cybersecurity risk, the programming and processes are more secure and safe than if they were to be used by people. The main reasoning behind this is that most cybersecurity breaches stem from human error. So, while RPA can introduce vulnerabilities to a firm, it is also used as a risk mitigation tool as fewer people are involved in processes that put firms at risk of breaches. Past studies support this data by stating that cybersecurity can be defined as a collection of tools, actions, training, risk management, assurance, security concepts, and technologies used to protect a firm's cyber environment (Eugen & Petrut, 2018). Rajan et al. (2021) further indicate that cybersecurity is used to help firms protect information integrity, confidentiality, and availability of information.

Based on the participants' experience, RPA can be used to ensure the privacy of the sensitive data of firms, whether the data be personal data or intellectual property of the firm. In addition to this, the data indicate that the risk surrounding cybersecurity and the security of information stems from the data itself since the bots' programming is safe. Additionally, the study supports this by stating that the use of RPA is not a risk, but the data and how the RPA program accesses the data is the risk their firm faces.

According to the conditions of POPIA, the storing of private information need to adhere to all the requirements put in place by regulatory bodies (POPIA, 2013). This includes collecting data and safely storing the data collected, and transferring data to other countries (POPIA, 2013). The study finds that one way to mitigate this access and data security risk is to have data fed to the RPA bots meaning that the firm stays in complete control of what data the bot can and cannot access. The alternative is to have the RPA robots 'fetch' the data in the location on the server, which adds to the cybersecurity and data protection risk faced by firms. Formosa et al. (2021) add to this by stating that with cybersecurity comes the element of a right to privacy which the study describes as a moral concept in which a person has the right to make their own decisions.

The data shows that some firms have set policies that need to be approved regarding data security and data protection before any RPA project can commence. Gartner (2021) finds that cyber vulnerabilities are among the main threats facing South African firms, which presents a significant challenge to the board of directors. Rajan et al. (2021) advise that the management of these cybersecurity challenges can be enhanced by good governance supported by the board of directors. This study also finds that some firms do not have the necessary information to contract policies as a preventative measure before implementing RPA. The policies are almost always reactive to events in the firms. This is mainly due to firms not being able to use a 'one size fits all' cybersecurity policy when they adopt RPA.

This study identified an additional measure that needs to be included in the governance of RPA, access management. The data shows that the RPA robots that access other systems need to be identified and verified before allowing access to the systems. This helps with cybersecurity in case of a breach and aids in data security. The study finds that firms can use the following as access management measures when they adopt RPA:

- Specific role-based access control governing the robot's access to the firm's data and infrastructure
- Credential validation when RPA robots log into systems

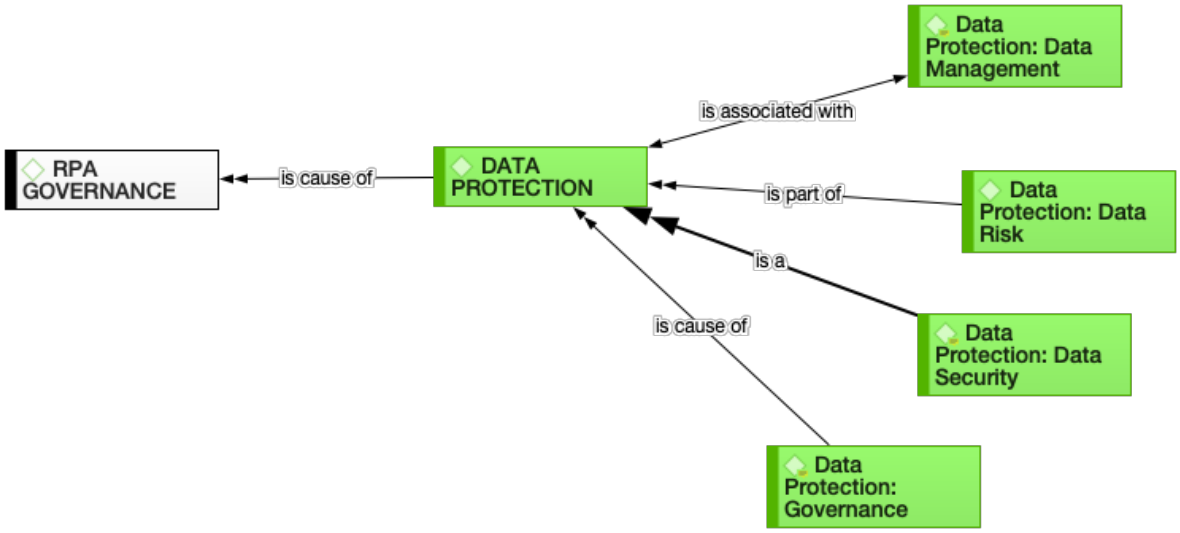
The credentials for the RPA programmes have to be stored in a secure location to prevent unauthorised people from accessing information and parts of the firm's systems that they are not allowed access to.

Based on the data from this section, the study concludes that cybersecurity is a primary tool used by firms to govern RPA. Cybersecurity in these firms depends directly on RPA security, data security and access management. In addition to this, the general governance principles applied to cybersecurity and the risk associated with cybersecurity play integral roles in ensuring that a firm's RPA software is secure.

5.3.2 The effect RPA has on data protection

The study section focused on how participants managed data protection and security when adopting RPA in their respective firms. The study finds that participants focussed on specific data management elements, data risk, securing the data and the governance of data which aligns with the regulation in South Africa, which is illustrated in Figure 7 below:

Figure 7: Elements of data protection concerning the governance of RPA



This study finds that firms need to know where information is to improve processes. In addition to firms knowing where data is stored, this study indicates that firms need to identify the data they will work with to manage the information effectively. One of the benefits experienced by firms that use RPA is that RPA is a data management tool firms can use. This is mainly due to the RPA program accessing and processing vast

volumes of data and presenting the workers with the outcome of the process. Past studies support the data by indicating that the data sources need to be clear and well-defined for data management to be effective. Research by van Bon et al. (2007) proposes a data administration process that includes defining the data, having a data inventory and maintaining a data catalogue.

This study finds that RPA needs similar governance to any other technology:

- Governance in terms of access, integration, and user roles
- Data governance and protection

When RPA programmes process large volumes of data, the proper governance of the data is essential. van Bon et al. (2007) support the data from the study by stating that it is the board's responsibility to ensure that all of the elements of data are controlled and that appropriate policies and standards are formulated for the management of the data in the firm. von Solms and von Solms (2006) state that data is the most valuable asset of any firm and that it is the board's responsibility to ensure that there is proper protection in place. Gartner (2021) also found that ITG and data governance are some of the top threats firms face, which present significant challenges to the board of directors. All of which are elements that need to be considered when firms deploy RPA as per the data gathered in the study.

This study finds that RPA processes can be an enabler of data security, and it is a tool to manage large volumes of data. Some firms use RPA as a data security measure. When firms deploy RPA, data gets deleted shortly after the process has run. This means that the data never permanently leave the original location where it is already secure. In addition to keeping data secure and having the appropriate policies and procedures to govern data in a firm, the Kovanen (2020) study supports this study by stating that data errors and incorrect data sets as risks that firms face when deploying RPA.

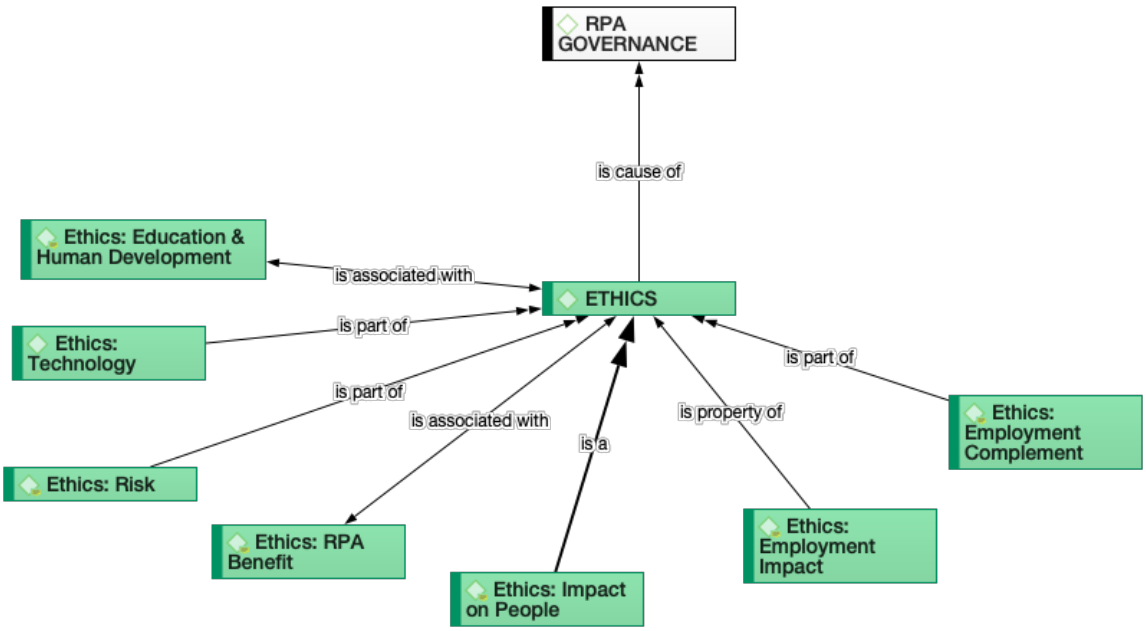
The data from this study further finds that data management is closely associated with data protection while data governance is a cause of data protection. On the other hand, data security is an exact form of data protection. Lastly, for firms to actively manage data, they need to identify the risks associated with gathering and storing data. These elements, (i) data management, (ii) data risk, (iii) data security and (iv)

data governance, form a holistic approach to help firms protect the data it processes, and since data is an integral part of RPA, this data protection function is a vital element of RPA governance.

5.4 The adoption of RPA and how South African firms can ethically manage the digitisation process when adopting RPA

This final section of the study focused on participants' experience regarding the ethical considerations, ethical challenges, and the impact on the workforce when the firm adopted RPA. The study finds that specific ethical considerations need to be made when firms want to deploy RPA: education and human development, the ethics behind the programming of the technology, the disadvantages of using RPA, and the advantages that contribute to an ethical firm. In addition to this, the study also finds that firms need to consider the impact RPA will have on people, how RPA will affect employment in the firm and whether RPA could be used as a complementary tool to employees rather than to reduce the workforce of the firm. These elements are illustrated in Figure 8 below:

Figure 8: Ethical considerations in relation to the governance of RPA



The study indicates that education and development need to be a key consideration for firms as this will lessen the impact RPA has on the workforce. The study finds that

firms need to invest in upskilling their staff to automate processes rather than outsourcing the skills to another firm. Additionally, the RPA strategy of firms should be to upskill employees to better use company resources which are seen as a critical success factor in implementing RPA. The research by Rajan et al. (2021), in support of this study, finds that the two determinants of governance are resources and capabilities and training and development. Furthermore, Rajan et al. (2021) indicate that when strong alliances and collaborations are experienced within firms, there is also a more significant opportunity for skills development and training.

This study highlights the importance of people in a firm when RPA is deployed. The study identifies that RPA risk is more people-related rather than implementation-related. Firms need to communicate to employees the exact purpose of adopting RPA openly. The leading reason firms need to focus on education and human development when they deploy RPA is to ensure that the impact on people is limited, which also highlights the impact on their employment. A study by Kirchmer (2017); Kovanen (2020) finds that one of the main challenges facing firms when implementing RPA is people-related risks which supports the data from this study.

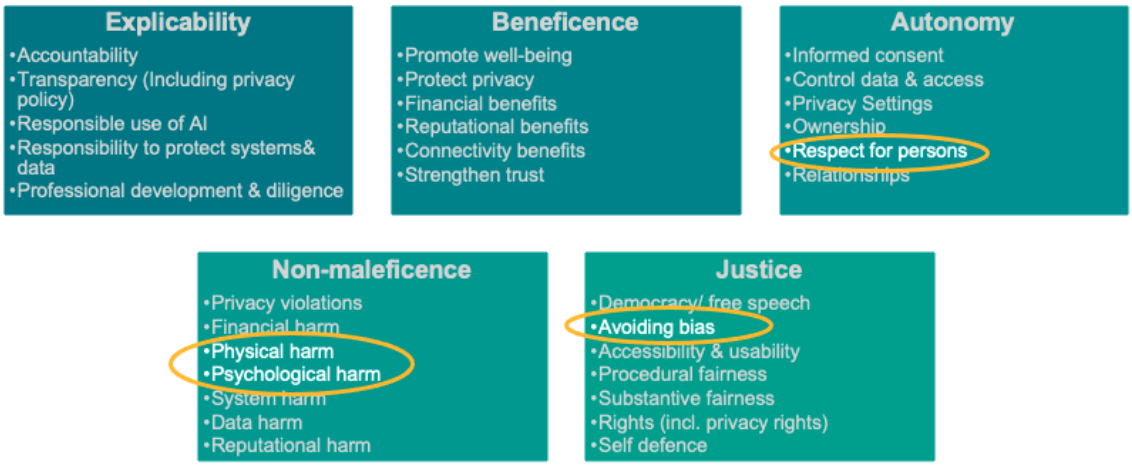
The data from this study shows that firms still need to consider the impact that RPA will have on the employees and the size of the workforce of firms. The study highlights an interesting observation: the firms may not be eliminating current jobs due to RPA, but they are not quickly replacing employees if they leave the firm. This means that even if it is not the firm's intention, some future jobs are still lost to the economy. While it is evident that the management of a firm needs to consider the impact on employment, it is also essential that employees make the same consideration. Part of this process is to ensure that firms communicate the purpose of RPA to the workforce and change employees' perspectives, and employees need to upskill and reskill, too, not be replaceable. Firms and employees need to understand that RPA can help reduce manual labour allowing employees to work on more value-adding work. Firms should ultimately aim to use RPA to enable employees to upskill rather than reduce the workforce.

This study indicates that people and technology should work together to help firms grow. The data shows that RPA can enable the workforce, highlighting how RPA can ultimately benefit the firm. People, technology, and processes are interconnected

when firms deploy RPA, and equal focus needs to be applied to all three of these elements to ensure the successful implementation for any firm. New technologies, business processes, and developing employees' digital skills can foster a culture that helps firms recognise their digital strategy faster than competitors (Orbik & Zozuľaková, 2019). Rajan et al. (2021) support the data from this study by stating that solid collaboration in firms positively impacts the development and deployment of the organisation's technological infrastructure.

One of the most significant risks highlighted by Chapter 2 of this study and the data collected, other than the impact RPA has on people and employment, is the biases that could stem from the development and implementation of RPA. This study highlights the same risks and concerns when implementing RPA. The data shows that considerations need to be made by firms for unbiased processes where tasks need to be built without prejudice against any race, sex or age. The data from this study indicate that the fundamental rights that apply to humans also need to apply to RPA. Furthermore, the use of RPA should not cause any mental or physical harm to employees. The appropriate considerations need to be made to ensure the safety of a firm's workforce. The robots used in RPA do not have value systems and cannot make people's decisions. Thus, it is the firm's responsibility to ensure that this is considered when developing and deploying RPA processes. Kovanen (2020) identifies technology risk as algorithm bias, data errors and incorrect implementation. Furthermore, these RPA programs can inherently have algorithm bias, where the programmer’s bias is evident in (i) the finding of the program or (ii) training data bias, where the training data has inherent discriminations and discrepancies (Beerbaum, 2020; Kovanen, 2020). In addition to this, Formosa et al. (2021) also highlights this bias and respect for persons and not causing phycological harm to people as some of the elements of ethics that a firm needs to consider. These elements are highlighted in Figure 9 below.

Figure 9: Five cybersecurity ethics principles (adapted)



Source: Adapted from Formosa et al., 2021

The data from this study indicates that the elements discussed in this section relate to firms' ethical considerations when adopting new technologies like RPA. The governance of RPA is dependent on the ethical considerations a firm needs to make. These ethical considerations depend on multiple individual elements: (i) education and human development, (ii) ethics associated with RPA, (iii) ethical risks associated with RPA, (iv) the impact on people, (v) the impact of RPA on employment and (vi) using RPA as a resource to assist the workforce rather than reducing it.

5.5 The expanded model for the governance of RPA by South African firms

Figure 3 in Chapter 2 showcases the basic model for RPA governance based on the research objectives of this study. So far in this chapter, these elements were explained in greater detail based on the study's findings. In this next section of the study, the aim is to conclude the results to develop an expanded model for the governance of RPA.

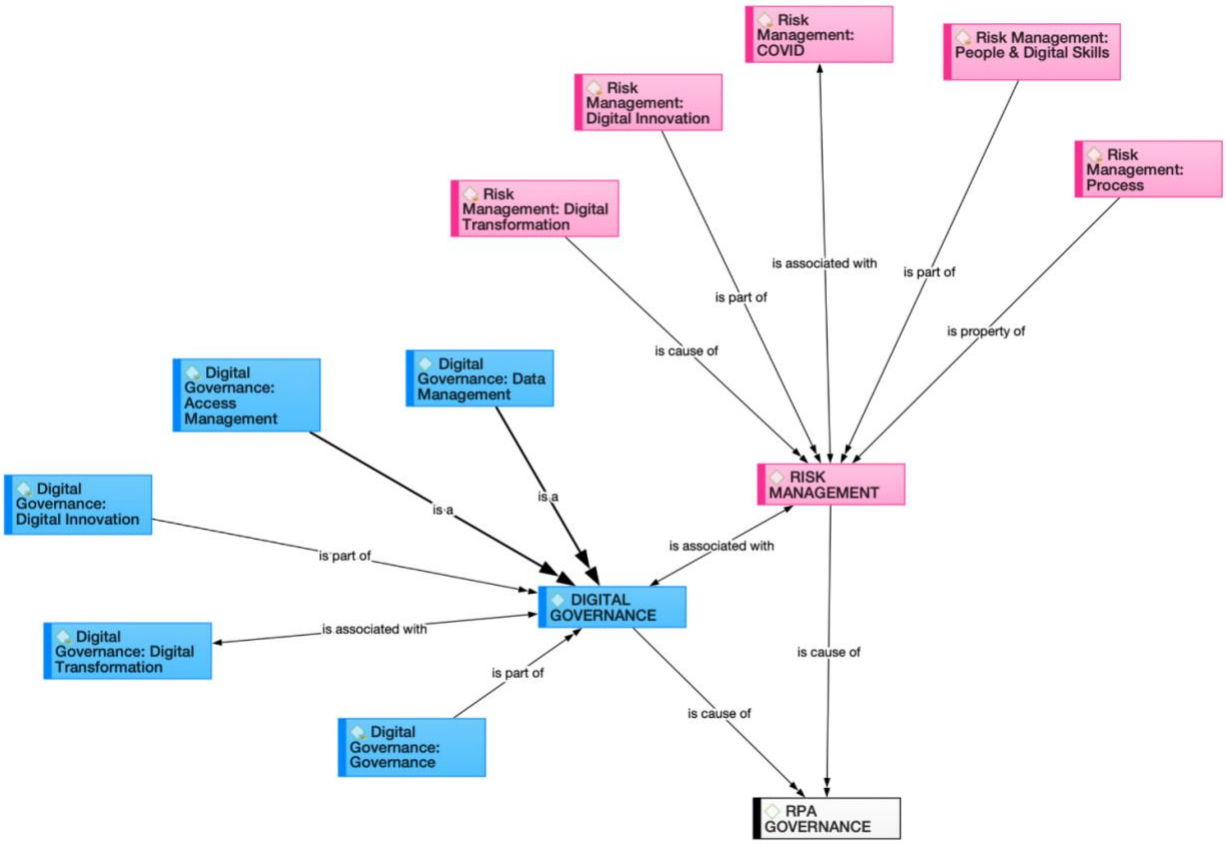
The first area of study for this research was focused on RPA adoption's impact on the ITG and risk management of a firm. The study found that the elements each have independent factors influencing and guiding firms to govern RPA when adopting the technology. Up to this point of the study, the focus has been on ITG. The expanded model for the governance of RPA will reference digital governance instead of ITG. This shift in language is more relevant to 21st century digital business. Firms today refer to digital innovation and not IT innovation, they reference digital transformation

and not IT transformation, the focus is thus not just on IT but multiple aspects of digital business. Firms, therefore, govern digital business and not IT business.

Based on the findings of this study, the digital governance policy of a firm that embraces RPA should include elements of data management, access management, general digital governance principles, the benefits derived from using RPA which refers to digital transformation, and the technology referring to innovation. In addition to this, firms also need to provide the risk associated with RPA and the vulnerabilities they could face when RPA is applied to business processes. The study finds that firms should consider process risk, people risk, pandemic risk, technology risk, and the effects of RPA that could help mitigate the risks they may face.

Figure 10 shows that even though digital governance and risk management are separate elements required for the governance of RPA, they are also related to one another and need to be addressed simultaneously in any policy about RPA.

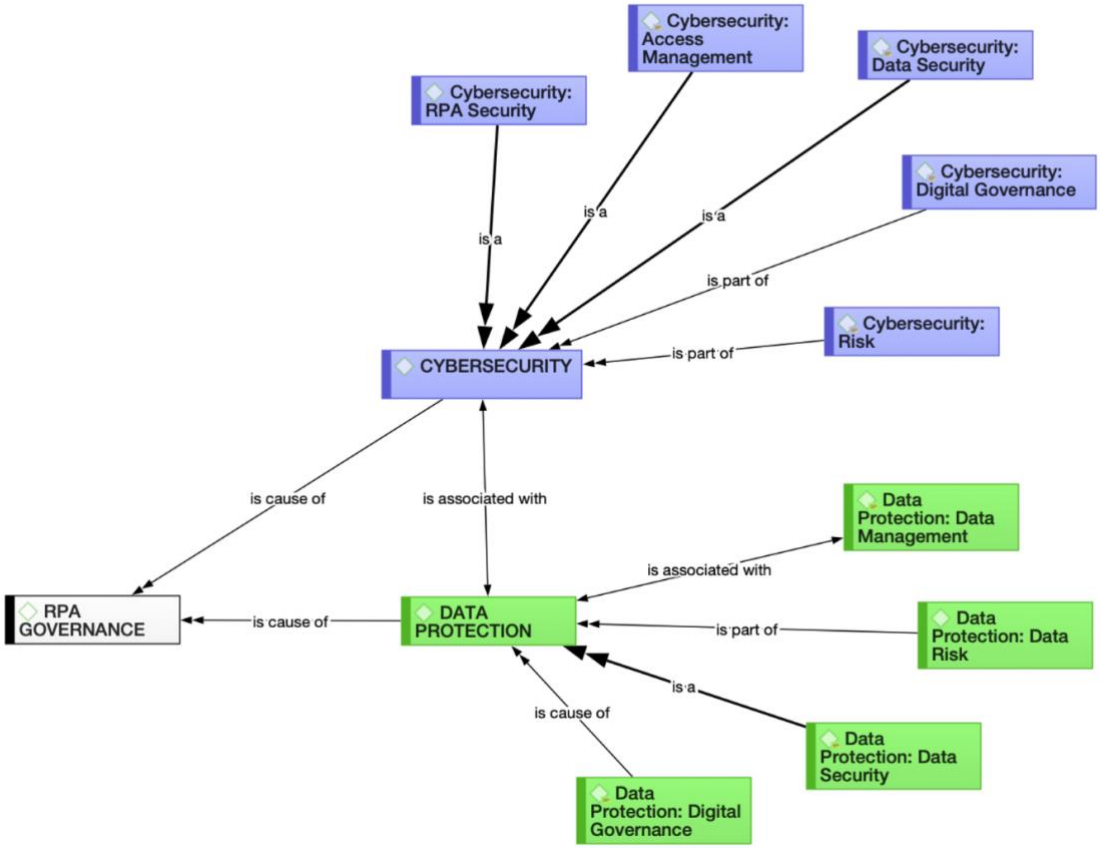
Figure 10: Digital governance and risk management elements for the governance of RPA



The next area of study was primarily concerned with cybersecurity and data protection and how these elements are impacted when firms adopt RPA. The study finds that cybersecurity policies should focus on the security of the RPA programs and platforms, data security and access management. In addition to this, the study also finds that general security governance principles should be applied to RPA and that identifying the risks associated with RPA should be identified and addressed accordingly. On the other hand, data protection policies for these firms should address data management processes, data security measures, identifying data risks and lastly, general data governance should be adopted as well.

Figure 11 indicates that even though cybersecurity and data protection are separate elements required for the governance of RPA, they are also related to one another and need to be addressed simultaneously in any policy about RPA.

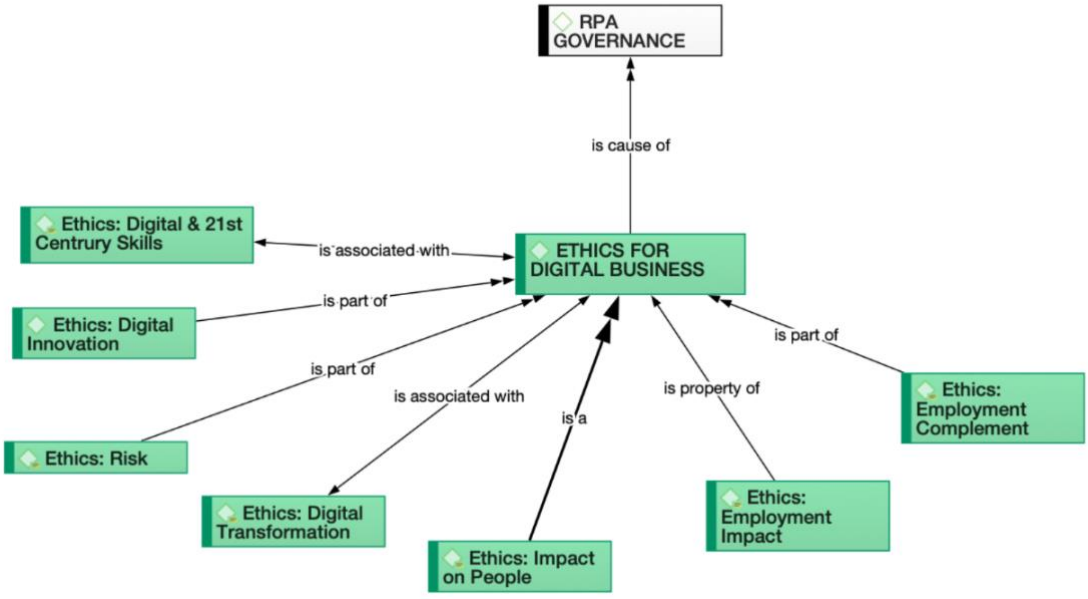
Figure 11: Cybersecurity and data protection measures for the governance of RPA



The final area of study was concerned with the ethical considerations that all firms need to address when adopting RPA. This study finds that there are multiple areas of ethics that firms need to address, including digital and 21st century skills of employees,

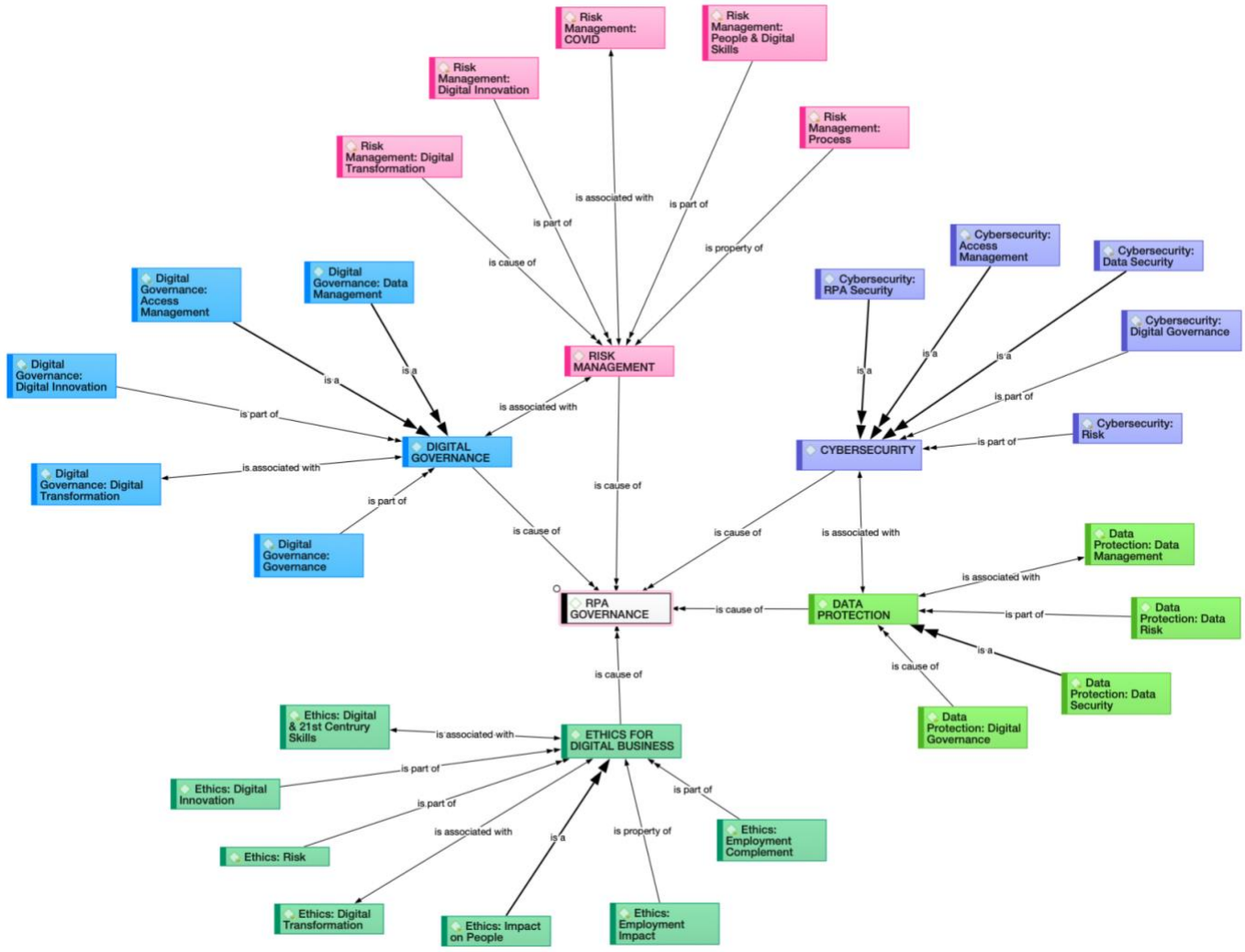
ethics associated with using RPA, ethical risks associated with using RPA, the impact that RPA has on people, the effect RPA has on employment and finally using RPA as a resource to assist the workforce rather than reducing it. These elements are illustrated in Figure 12 below.

Figure 12: Digital ethics for the governance of RPA



Adding all the elements and their focus areas provides a holistic governance overview of the considerations that need to be addressed when developing and implementing RPA in any firm in South Africa. The below model is an expanded model that was illustrated in Figure 3. This governance model of RPA demonstrated below summarises the findings of this paper in a single holistic view.

Figure 13: An expanded model for RPA governance in South African digital business



This multifaceted model for the governance of RPA shows that firms need to consider multiple elements from digital governance and risk management to cybersecurity and data protection and digital ethical aspects when they deploy RPA. This model should form the basis of RPA governance for any firm within South Africa when they adopt RPA.

The model identifies that firms need digital and 21st-century skills to adequately govern RPA. van Laar et al. (2017) finds that people need core skills which include technical, communication, information management, collaboration, critical thinking, creativity, and problem-solving as part of the digital transformation journey. People also need contextual skills like ethical awareness, flexibility, cultural awareness, self-direction and lifelong learned when they embark on the digital transformation journey (van Laar et al., 2017). These same skills are required to adopt and govern RPA.

Chapter 6: Governance principles of RPA

6.1 Chapter introduction

The current body of literature does not adequately address the policies and procedures that need to be in place to ensure good governance when firms in South Africa decide to adopt RPA. Firms in retail, manufacturing banking and financial services, investment holdings and software developers are market leaders concerning the adoption of RPA in South Africa. This study aimed to address this by researching the governance principles that need to be in place for firms to implement RPA. This study aimed to answer the main research question to determine how corporate governance should adopt concerning the adoption and use of RPA. To start answering the main research question, the study focussed broadly on three elements of governance that are affected when firms adopt RPA. These elements are (i) digital governance and risk management, (ii) cybersecurity and data protection, and (iii) the digital ethical considerations firms need to address when they deploy RPA software.

The aggregated model for RPA governance, Figure 13, was developed to showcase the elements of governance that firms need to consider when they adopt RPA. This model illustrates that RPA governance is multifaceted and that firms need to ensure that the RPA governance policy addresses all aspects of these elements.

6.2 Corporate governance principles for using RPA by firms in South Africa

Corporate governance in South Africa is an advanced field. Still, the information currently in the literature does not adequately address the governance principles that need to be in place specifically for the adoption of RPA by South African firms. The following principles are recommended by the researcher, based on the expanded model for the governance of RPA developed by this study, as guidance for the governance of RPA when South African firms adopt RPA:

- Principle 1: For the effective governance of RPA, firms should incorporate elements of digital governance, risk management, cybersecurity, data protection and digital ethics in the governance policy.

- Principle 2: The effective governance of RPA should include access management and standard elements of digital governance.
- Principle 3: The effective governance of RPA should incorporate developing people and digital skills and process risk management.
- Principle 4: The effective governance of RPA should contain elements of RPA cybersecurity principles and cybersecurity risk management.
- Principle 5: The effective governance of RPA should include elements of data protection, data management and data security.
- Principle 6: For the ethical governance of RPA digital business should incorporate digital and 21st-century skills for employees.
- Principle 7: Ethical RPA governance should also recognise the positive and negative impact that RPA will have on employees and how the technology could be used as an employment complement in forms of collaborative technology.

6.3 Recommendations for future research

This study only focused on three areas of governance: digital governance and risk management, cybersecurity and data protection, and the digital ethical considerations that firms need to address in adopting RPA.

Elements highlighted by the data but not discussed in this paper include the effect that change management has on the governance of RPA and the relationship between governing RPA and business growth. Therefore, it is suggested that further research be conducted to determine the effect that change management has on the governance of RPA and determine what relationship exists between business growth and RPA governance. Further research can also be conducted on other elements of governance and how they are influenced when firms in South Africa adopt RPA. These elements can include internal control, operational risks and sustainability and scalability.

The RPA governance model developed in this study could be used as the foundation for the development of regulatory technology (RegTech) and the technology used by supervisory agencies (Suptech) as this model can be easily adapted to incorporate any other digital business tools. The application of this model to other digital business

tools is not covered by this study as it does not relate to the objectives developed in Chapter 1 of this paper.

References

Asatiani, A., Kämäräinen, T., & Penttinen, E. (2019). *Unexpected problems associated with the federated IT governance structure in robotic process automation (RPA) deployment* Aalto University]. Helsinki. http://urn.fi/URN:ISBN:978-952-60-6899-2

Beerbaum, D. (2020). Artificial intelligence ethics taxonomy-robotic process automation (RPA) as

business case. *The European Research Journal*(Special Issue 'Artificial Intelligence& Ethics' European Scientific Journal). https://doi.org/http://dx.doi.org/10.2139/ssrn.3834361

Bergeron, F., Croteau, A.-M., Uwizeyemungu, S., & Raymond, L. (2015). *IT governance theories and the reality of SMEs: bridging the gap* 2015 48th Hawaii International Conference on System Sciences, https://www.researchgate.net/publication/283800961

Buckby, S. (2011). *Exploring the role of the governing body (board) in information technology governance : a study of Australian universities* [PhD, Queensland University of Technology]. Queensland, Australia. https://eprints.qut.edu.au/43881/

Creswell, J. W. (2013). *Qualitative inquiry & research design*. Vicki Knight.

Davis, J. H., Schoorman, F. D., & Donaldson, L. (1997, January 1997). Toward a stewardship theory of management. *Academy of Management Review, 12*(1), 20-47. https://doi.org/10.5465/AMR.1997.9707180258

de Bruyn, M. (2014). The protection of personal information (POPI) act - Impact on South Africa. *International Business & Economic Research Journal (IBER), 13*(6), 1315 - 1340. https://doi.org/https://doi.org/10.19030/iber.v13i6.8922

Debreceny, R. S. (2013). Research on IT governance, risk, and value: challenges and opportunities. *Journal of Information Systems, 27*(1), 129-135. https://doi.org/10.2308/isys-10339

Dudovskiy, J. (2018). *Interpretivism (interpretivist) research philosophy*. Business Research Methodology. Retrieved July from https://research-methodology.net/research-philosophy/interpretivism/

Eugen, P., & Petrut, D. (2018). Exploring the new era of cybersecurity governance. *"Ovidius" University Annals, Economic Sciences Series, 18*(1), 358-363. https://www.researchgate.net/profile/Petac-Eugen-2/publication/330652052_Exploring_the_New_Era_of_Cybersecurity_Governance/links/5c4c437b299bf12be3e513d6/Exploring-the-New-Era-of-Cybersecurity-Governance.pdf

Formosa, P., Wilson, M., & Richards, D. (2021). A principlist framework for cybersecurity ethics. *Computers & Security, 109*. https://doi.org/10.1016/j.cose.2021.102382

Gartner. (2021). Gartner identifies data governance and cyber security as top risks for 2021. *IQ: The RIM Quarterly, 2021*(June), 46-47. http://web.b.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=8&sid=74dcac07-4844-4302-bb20-5504d138c71d%40pdc-v-sessmgr02

Hardy, G. (2006). Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. *Information Security Technical Report, 11*(1), 55-61. https://doi.org/10.1016/j.istr.2005.12.004

Hartmann, C., & Carmenate, J. (2021, April 2021). Academic research on the role of corporate governance and IT expertise in addressing cybersecurity breaches: Implications for practice, policy and research. *American Accounting Association*(Current Issues in Auditing 2021). https://doi.org/https://doi.org/10.2308/CIIA-2020-034

Huang, F., & Vasarhelyi, M. A. (2019). Applying robotic process automation (RPA) in auditing: A framework. *International Journal of Accounting Information Systems, 35*. https://doi.org/10.1016/j.accinf.2019.100433

IODSA. (2016). King IV®: Report on corporate governance in South Africa. https://www.adams.africa/wp-content/uploads/2016/11/King-IV-Report.pdf

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm- managerial behavior, agency costs and ownership structure. *Journal of Financial Economics, 3*(4), 305-360. https://doi.org/https://doi.org/10.1016/0304-405X(76)90026-X

Kirchmer, M. (2017). *Robotic process automation - pragmatic solution or dangerous illusion?* BTOESInsignts. Retrieved May from https://insights.btoes.com/risks-robotic-process-automation-pragmatic-solution-or-dangerous-illusion

Kovanen, A. (2020). *Risks of intelligent automation and their impact on internal audit* [Master's Thesis, Tampere University]. https://trepo.tuni.fi/bitstream/handle/10024/121440/KovanenAnni.pdf?sequence=2

Lobschat, L., Mueller, B., Eggers, F., Brandimarte, L., Diefenbach, S., Kroschke, M., & Wirtz, J. (2021). Corporate digital responsibility. *Journal of Business Research, 122*, 875-888. https://doi.org/10.1016/j.jbusres.2019.10.006

Lowes, P., Cannata, F. R. S., Chitre, S., & Barkham, J. (2017). Automate this: The business leader's guide to robotic and intelligent automation. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/process-and-operations/us-sdt-process-automation.pdf

Maroun, W., & Cerbone, D. (2020). *Corporate governance in South Africa*. De Gruyter Oldenbourg.

Orbik, Z., & Zozuľaková, V. (2019). Corporate social and digital responsibility. *Management Systems in Production Engineering, 27*(2), 79-83. https://doi.org/10.1515/mspe-2019-0013

Pereira, R., & da Silva, M. (2012). IT governance implementation: The determinant factors. *Communications of the IBIMA*, 1-16. https://doi.org/10.5171/2012.970363

Rajan, R., Rana, N. P., Parameswar, N., Dhir, S., Sushil, & Dwivedi, Y. K. (2021). Developing a modified total interpretive structural model (M-TISM) for organizational strategic cybersecurity management. *Technological Forecasting and Social Change, 170*. https://doi.org/10.1016/j.techfore.2021.120872

Rutaganda, L., Bergstrom, R., Jayashekhar, A., Jayasinghe, D., & Ahmed, J. (2017). Avoiding pitfalls and unlocking real business value with RPA. *The Capco Institute Journal of Financial Transformation, 46*(11), 104 - 115. https://www.capco.com/-/media/CapcoMedia/Capco-Institute/Journal-46/JOURNAL46_full_web.ashx#page=104

Smits, D., & van Hillegersberg, J. (2018). The continuing mismatch between IT governance maturity theory and practice: a new approach. *Procedia Computer Science, 138*(2018), 549-560. https://doi.org/10.1016/j.procs.2018.10.075

Syed, R., Suriadi, S., Adams, M., Bandara, W., Leemans, S. J. J., Ouyang, C., ter Hofstede, A. H. M., van de Weerd, I., Wynn, M. T., & Reijers, H. A. (2020). Robotic process automation: Contemporary themes and challenges. *Computers in Industry, 115*. https://doi.org/10.1016/j.compind.2019.103162

van Bon, J., De Jong, A., kolthof, A., Pieper, M., Tjassing, R., van der Veen, A., & Verheijen, T. (2007). *Foundations of IT service management based on ITIL V3* (J. Wilkinson, Ed. Third ed.). Van Haren Publishing, Zaltbommel.

van Laar, E., van Deursen, A. J. A. M., van Dijk, J. A. G. M., & de Haan, J. (2017). The relation between 21st-century skills and digital skills: A systematic literature review. *Computers in Human Behavior, 72*, 577-588. https://doi.org/10.1016/j.chb.2017.03.010

von Solms, R., & von Solms, S. H. (2006). Information security governance: A model based on the direct–control cycle. *Computers & Security, 25*(6), 408-412. https://doi.org/10.1016/j.cose.2006.07.005

Whiting, R., & Pritchard, K. (2017). Digital ethics. In *Sage Handbook of Qualitative Research in Business and Management*. Birkbeck Institutional Research Online. https://eprints.bbk.ac.uk/id/eprint/15623/

Wu, S. P.-J., Straub, D. W., & Liang, T.-P. (2015, June 2015). How information technology governance mechanisms and strategic alignment influence organizational performance. *MIS Quarterly, 39*(2), 497-518. https://www.jstor.org/stable/10.2307/26628363

Yuvaraja, D. (2018). A study of robotic process automation: Use cases today for tomorrow's business. *International Journal of Computer Techniques, 5*(6), 12-18. http://www.ijctjournal.org/Volume5/Issue6/IJCT-V5I6P3.pdf

Zhen, J., Xie, Z., & Dong, K. (2021). Impact of IT governance mechanisms on organizational agility and the role of top management support and IT ambidexterity. *International Journal of Accounting Information Systems, 40*. https://doi.org/10.1016/j.accinf.2021.100501

APPENDIX A: Codes consolidation matrix

Color	Category	Sub-Category	Codes
●	Business Growth	Business Growth: Business	Business Growth Business Strategy Committee Competition Disruption Income Insurance KPI Money Save No Business Growth No scalable ROI RPA as a Service RPA Strategy SAAS Scalability Service Provider Success
		Business Growth: Process	Process
		Business Growth: RPA	RPA
		Business Growth: RPA Benefit	Competitive Advantage Data Driven Decision Making Data from RPA Decision Making Digitize Monetise Data RPA Value Solution Automation Capacity Increase Gap Optimization RPA Benefit RPA Effect Reporting

Color	Category	Sub-Category	Codes
			RPA Workload RPA work hours
		Business Growth: RPA Disadvantage	Costly RPA Drawback
		Business Growth: Technology	Technology
●	Change Management	Change Management: People	Ambassador Awareness Challenge Change Management Collaboration Comfort Communication Concern Culture expectations Fear Frustration Human Beliefs Human Judgement Misunderstanding No Trust Resistance Support Uncertainty Unknown Wary Change

Color	Category	Sub-Category	Codes
		Change Management: Risk	Risk
		Change Management: RPA	RPA
		Change Management: RPA Benefit	RPA Benefit
		Change Management: Technology	Technology Change
●	Cybersecurity	Cybersecurity: Access Management	Access Security Authenticate Authorisation Password Vault RPA Access Service Accounts User Access User Role Validation Virtual access
		Cybersecurity: Data Security	Penetration testing Firewall Hacking Security Lower Cyber Threat
		Cybersecurity: Governance	Cybersecurity Cybersecurity Test ISO Parameter Security Platform Security
		Cybersecurity: Risk	Cybersecurity Risk
		Cybersecurity: RPA Security	RPA Security
		Cybersecurity: Technology	AI Cloud HTTP HTTPS
●	Data Protection	Data Protection: Business	Business

Color	Category	Sub-Category	Codes
		Data Protection: Data Management	Data Destruction Data error Data Processing Integration no data processing RPA Output Sensitive Data Identification Temporary Data Backup of Tasks Data Data Storage
		Data Protection: Data Risk	Data Risk
		Data Protection: Data Security	Data Protection Data Transportation Encryption Information Information Security Off Premise Data Access Off Premise Data Security Data Encryption Cyber Threats
		Data Protection: Governance	Data governance and laws POPIA Privacy Right to Privacy Confidentiality
●	Ethics	Ethics: Education & Human Development	Low Skill Not trainable Skill Training
		Ethics: Employment Complement	Employment Complement Employment Growth Employment Shift Employment Strategy No Employment Change
		Ethics: Employment Impact	Employment displacement People

Color	Category	Sub-Category	Codes
		Ethics: Ethics	Ethical Dilemma No Ethical Challenge
		Ethics: Impact on People	Fairness Fundamental Rights Human Safety Human Value Human Values Impact Intention Knowledge Loss Low Salary Management Manager Performance Measurement Transparency Value Salary South Africa Purpose Realisation
		Ethics: Risk	SA Unions
●	Ethics	Ethics: RPA Benefit	Development Digital Workforce Productivity Resource optimization RPA as person
		Ethics: RPA Disadvantage	Not enough people Unemployment Employment Loss Human Bias No Value Add RPA Bias RPA no value system RPA not a Solution
		Ethics: Technology	Technology
●	IT Governance	IT Governance: Access Management	Credentials
		IT Governance: Data Management	Data Management

Color	Category	Sub-Category	Codes
		IT Governance: Governance	Accountability Accounting Audit Best Practice Centre of Excellence CIO Controls Controls after Automation Controls Before Automation Controls Lacking Corporate Digital Responsibility Corporate Governance Corporate Responsibility Country Specific CSO CTO Environmental Social Governance Existing Policy Federated ITG Fragmented ITG Governance Governance before Automation Governance Challenge IT Framework ITG ITG Improvement ITG theories Legacy ITG No Centre of Excellence Overarching ITG Policy Preventative Controls Principle Process Documentation Protective Controls Regulation

Color	Category	Sub-Category	Codes
			RPA testing Segregation of Duties Segregation of Tasks Testing Environment User Acceptance Testing Virtual Infrastructure
●	IT Governance	IT Governance: RPA	Implementation On Premise RPA Design Instruction No RPA Limit RPA not intelligent automation
		IT Governance: RPA Benefit	Internal Use of RPA Silent Recording
		IT Governance: Technology	Equipment ERP Infrastructure IT Load Balancer Machine Learning no IT challenge Not in IT RPA is software Technology Not Priority Redirect Digital Workforce Slow
●	Risk Management	Risk Management: COVID	Work From Home
		Risk Management: People	Fraud Malicious Intent Deliberate Sabotage

Color	Category	Sub-Category	Codes
		Risk Management: Process	Complex Complex Process Monitoring Process Defined before RPA Process Selection Simplicity Duplication Operational Risk Continued Continued Checks Human Intervention Input Accuracy Process Inefficiencies Process Loss Process Risk Oversight RPA Process Process Process Management Reactive Process Repetitive process
		Risk Management: Risk	Risk Appetite Risk Assessment Risk Management Risk register Failure Incorrect Implementation no IT Risk Restrictions Proactive

Color	Category	Sub-Category	Codes
●	Risk Management	Risk Management: RPA Benefit	Anomaly Detection Error Logs Error Reduction Exception Management Human Error Improvement No Human Intervention Process accuracy Process Efficiency Robot Segregation Standardisation Risk Mitigation Alert Exposure Limitation Reliability
		Risk Management: Technology	RPA Risk Connectivity Risk IT risk Vulnerability Not on Physical Machines

APPENDIX B: Participant information sheet



UNIVERSITY OF THE
WITWATERSRAND,
JOHANNESBURG

1 Jan Smuts Avenue
Johannesburg
2000

PARTICIPANT INFORMATION SHEET

Dear Sir / Madam,

My name is Anri Nortje, a Masters student in Management in the field of Digital Business at the University of the Witwatersrand in Johannesburg. As part of my studies, I have to undertake a research project, currently titled: "Corporate governance for robotic process automation by South African firms". The aim of this research project is to explore the best practices that need to be adhered to by South African firms when they implement RPA in terms of IT governance and risk management, cybersecurity, and data protection as well as the ethical digitalisation of the firm.

As part of this project, I would like to invite you to take part in an interview. This activity will take around sixty minutes. With your permission, I would also like to record the interview using a voice recording application on a cellphone.

You will not receive any direct benefits from participating in this research, and there are no disadvantages or penalties for not participating. You may withdraw at any time or not answer any question if you do not want to. The interview will be completely confidential, and anonymous to the public, as I will not publish your name or any identifying information, and the information you give to me will be held securely and only used for academic publication. I will use a pseudonym (false name) to represent your participation in my final research report. If you experience any distress or discomfort at any point in this process, we will stop the interview or resume another time.

If you have any questions at any time during this research process, feel free to contact me or my supervisor using the details listed below. This study will be written up as a research report which will be available online through the university library website. If you wish to receive a summary of this report, I will be happy to send it to you. If you have any concerns or complaints regarding the ethical procedures of this study, you are welcome to contact the University Human Research Ethics Committee (Non-Medical), telephone +27(0) 11 717 1408, email Shaun.Schoeman@wits.ac.za.

Yours sincerely,
Name: Anri Nortje

Anri Nortje, oberholzeranri@gmail.com, 073 447 5767
Dr Lucienne Abrahams, luciennesa@gmail.com, 082 569 7675

APPENDIX C: Informed consent

Interview: Informed Consent Form

Research title: Corporate governance for robotic process automation by South African firms

Researcher's name: Anri Nortje

I ……. agree to participate in this research project. The research has been explained to me and I understand what my participation will involve.

I agree that my participation will remain anonymous	YES	NO	(please circle)
I agree that the researcher may use anonymous quotes in his research report	YES	NO	
I agree that the interview may be audio recorded	YES	NO	
I agree that the information I provide may be used anonymously by other researchers following this study	YES	NO	

…… (participant's signature)

…… (name of participant)

…… (date)

…….(researcher's signature)

Anri Nortje…….(name of researcher)

…….(date)

APPENDIX D: Interview guide

IT Governance and Risk Management

1. How has the use of Robotic Process Automation (RPA) influenced the conversation and decision-making in the IT governance structure in your organisation?
2. What have been your biggest impact and governance challenges with respect to RPA adoption?
3. How has RPA affected the day-to-day risk management in your organisation?
4. In which ways has RPA influenced a change in risk management strategy?

Cybersecurity and Data Protection

1. Which aspects of cybersecurity were part of the initial design and implementation of RPA in your organisation? What cybersecurity matters were considered and why? If cybersecurity was not considered, why not?
2. How does your organisation manage data protection and data security in the context where RPA technologies access and process data?
3. What have been the major challenges in cybersecurity and data protection/security stemming from the use of RPA? How did the business overcome these challenges?

Ethics

1. In your experience, what ethical considerations need to be addressed when organisations deploy new technologies, specifically RPA?
2. What have been the major ethical challenges arising from the use of RPA? How was this managed and addressed?
3. Has there been / or do you anticipate any job losses because of RPA adoption?

Closing Question

1. Based on your experience, what corporate governance good practice principles should be applied when organisations like yourselves deploy RPA?

APPENDIX E: 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/DB1171378/417
This certificate is only valid with a legitimate ethics protocol number and signed by the Researcher (below).

Project title	Corporate governance of robotic process automation by South African firms
Investigator / Researcher	Mrs Anri Nortje
Nature of Project	MM (Digital Business)
Decision of the Committee	Approved, provided stakeholders and participants are guaranteed anonymity and 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

14 FEBRUARY 2022
Date: