



AN EMPIRICAL INVESTIGATION INTO THE INFORMATION MANAGEMENT SYSTEMS AT A  
SOUTH AFRICAN FINANCIAL INSTITUTION

by

RIDOH ADONIS

Dissertation submitted in partial fulfilment of the requirements of the degree Master of Technology:  
Business Administration in the Faculty of Commerce at the Cape Peninsula University of  
Technology

Supervisor: Dr Bethuel Sibongiseni Ngcamu  
Qualifications: PHD, DTech

Cape Town campus  
Date submitted: June 2016

**CPUT copyright information**

The dissertation/thesis may not be published either in part (in scholarly, scientific or technical journals), or as a whole (as a monograph), unless permission has been obtained from the University

## DECLARATION

I, Ridoh Adonis, declare that the contents of this dissertation/thesis represent my own unaided work, and that the dissertation/thesis has not previously been submitted for academic examination towards any qualification. Furthermore, it represents my own opinions and not necessarily those of the Cape Peninsula University of Technology.

A handwritten signature in black ink, appearing to read 'Ridoh Adonis'. The signature is written in a cursive style with a large, circular flourish at the beginning.

R Adonis

14 June 2016

## **ABSTRACT**

The study has been triggered by the increase in information breaches in organisations. Organisations may have policies and procedures, strategies and systems in place in order to mitigate the risk of information breaches; however, data breaches are still on the rise. Governments across the world have or are putting in place laws around data protection which organisations have to align their process, strategies and systems to. The continuous and rapid emergence of new technology is making it even easier for information breaches to occur. In particular, the focus of this study is aimed at the information management systems in a selected financial institution in South Africa. Based on the objectives, this study: explored the shortfalls of information security on a South African financial institution; investigated whether data remains separate while privacy is ensured; investigated responsiveness of business processes on information management; investigated the capability of systems on information management; investigated the strategies formulated for information management and finally, investigated projects and programmes aimed at addressing information management. Quantitative, as well as qualitative analysis, was employed whereby questionnaires were sent to employees who were employed at junior management positions. Semi-structured in-depth interviews were self-administered whereby the researcher interviewed senior management at the organisation. These senior managers from different value chains are responsible for implementing information management policies and strategy.

The results showed that like many organisations, this institution has policies and procedures in place dealing with information management. Data analysis revealed that employees at the institution are not trained on these policies and procedures and, therefore, do not fully understand the requirements and impacts. This, therefore, leaves a big gap for information breaches. The thesis principally concludes that there are meaningful projects and programmes that the organisation can implement to improve the state of information security and information management. The managerial implications impact senior management first. The findings will enable senior managers to construct projects and programmes with their teams to implement the recommendations whilst minimizing the risks of information management breaches across the people aspect, technology systems as well as general processes. This study will improve the understanding of information management at the organisation as well as other similar organisations. The findings also contribute to the growing body of literature on information management in South Africa.

## **ACKNOWLEDGEMENTS**

I would first like to thank my thesis advisor, Dr. Bethuel Sibongiseni Ngcamu of the Faculty of Commerce at Cape Peninsula University of Technology. Dr. Ngcamu was always available to guide me with my research or writing. He consistently allowed this study to be my own work but steered me in the right direction when needed.

Finally, I must express my very profound gratitude to three women who all played a part in my journey of achieving this academic accomplishment. My aunt, Samsoeniesa Behardien who nurtured and guided me during my early schooling career, my mother, Faiza Adonis who made it possible for me to further my studies after high school, and lastly, my wife, Sideeqah Adonis for providing me with unfailing support and continuous encouragement throughout the process of researching and writing this thesis.

Author

Ridoh Adonis

## GLOSSARY

<b>Acronym</b>	<b>Term</b>
BCP	Business Continuity Planning
BR	Business Risk
DGC	Data Governance Council
ETL	Extract Transform and Load
FTP	File Transfer Protocol
ITRC	Information Technology Risk Committee
JV	Joint Venture
NCAA	National Credit Act Amendment
PCI	Payment Card Industry
POPI Act	Protection of Personal Information Act
SFTP	Secure File Transfer Protocol
USB	Universal Serial Bus
WIGs	Wildly Important Goals

## Table of Contents

<b>CHAPTER ONE: INTRODUCTION.....</b>	<b>5</b>
1.1    PROBLEM STATEMENT.....	6
1.2    RESEARCH AIM AND OBJECTIVES .....	6
1.3    RESEARCH QUESTIONS.....	7
1.4    PRELIMINARY LITERATURE REVIEW.....	7
1.5    RESEARCH OUTLINE .....	9
<b>CHAPTER TWO: INFORMATION MANAGEMENT IN A FINANCIAL INSTITUTION: AN INTERNATIONAL INSTITUTION .....</b>	<b>11</b>
2.1    INTRODUCTION.....	11
2.2    INFORMATION PRIVACY .....	11
2.3    INFORMATION SECURITY SYSTEMS .....	12
2.4    DATA BREACHES: TECHNOLOGY VS. EMPLOYEE.....	14
2.5    DATA BREACHING INCIDENTS AND SECURITY PROGRAMMES.....	15
2.6    EMPLOYEE BEHAVIOUR RELATING TO INFORMATION MANAGEMENT AND SECURITY.....	17
2.7    INFORMATION RISK ASSESSMENT AND MANAGEMENT.....	20
2.8    HANDLING INFORMATION .....	21
2.9    INTERNATIONAL LEGISLATION ON INFORMATION MANAGEMENT .....	23
2.10   INFORMATION GOVERNANCE OUTSOURCING.....	24
2.11   SUMMARY.....	26
<b>CHAPTER THREE: INFORMATION MANAGEMENT IN A FINANCIAL INSTITUTION: A SOUTH AFRICAN INSTITUTION .....</b>	<b>28</b>
3.1    INTRODUCTION.....	28
3.2    CORPORATE GOVERNANCE.....	28
3.3    LEGISLATIVE FRAMEWORK ON INFORMATION MANAGEMENT .....	30
3.4    INFORMATION STRUCTURE AND USE IN SOUTH AFRICAN ORGANISATIONS.....	34
3.5    INFORMATION MANAGEMENT POLICIES AT A SELECTED SOUTH AFRICAN FINANCIAL INSTITUTION .....	37
3.6    SUMMARY.....	41
<b>CHAPTER FOUR: RESEARCH DESIGN AND METHODOLOGY .....</b>	<b>43</b>
4.1    INTRODUCTION.....	43

4.2	FOCUS OF THE STUDY .....	43
4.3	RESEARCH OBJECTIVES.....	43
4.4	RESEARCH QUESTIONS.....	44
4.5	RESEARCH APPROACH .....	44
4.6	SAMPLING PROCEDURE AND DESCRIPTION OF THE SAMPLE.....	45
4.6.1	<i>Population</i> .....	45
4.6.2	<i>Sampling for the quantitative research method</i> .....	46
4.6.3	<i>Sampling for the qualitative research method</i> .....	46
4.7	DATA COLLECTION .....	47
4.8	PILOTING.....	48
4.9	QUANTITATIVE DATA ANALYSIS.....	49
4.10	QUALITATIVE DATA ANALYSIS .....	53
4.11	RESEARCH RELIABILITY AND VALIDITY.....	54
4.12	ETHICAL CONSIDERATIONS .....	54
4.13	SUMMARY.....	55
<b>CHAPTER FIVE: DATA PRESENTATION AND ANALYSIS (A) .....</b>		<b>56</b>
5.1	INTRODUCTION.....	56
5.2	RELIABILITY TESTING.....	56
5.3	FACTOR ANALYSIS.....	57
5.4	RESEARCH FINDINGS AND ANALYSIS.....	57
5.5	HYPOTHESIS TESTING .....	72
5.6	CORRELATIONS.....	80
5.7	SUMMARY.....	89
<b>CHAPTER SIX: DATA PRESENTATION AND ANALYSIS (B).....</b>		<b>90</b>
6.1	INTRODUCTION.....	90
6.2	IN-DEPTH INTERVIEW FINDINGS .....	90
6.2.1	WHAT PLANS DO HAVE TO ENSURE THAT EMPLOYEES DO NOT BREACH INFORMATION IN THIS ORGANISATION?.....	90
6.2.2	DO YOU HAVE POLICIES IN THIS INSTITUTION DEALING WITH INFORMATION MANAGEMENT? Yes/No.....	91
6.2.3	IF YES, ARE THEY RESPONSIVE OR ALIGNED TO NATIONAL LEGISLATIONS? .....	91

6.2.4	WHAT ARE THE OPPORTUNITIES AND CHALLENGES BROUGHT BY THIS POLICY? .....	92
6.2.5	WHAT ORGANISATIONAL PLANS ARE IN PLACE TO ENSURE THAT YOUR KEY STAKEHOLDERS (EMPLOYEES, VENDORS, ETC.) DO NOT BREACH INFORMATION? .....	93
6.2.6	WHAT TOOLS DO YOU HAVE IN PLACE TO ENSURE THAT YOUR KEY STAKEHOLDERS DO NOT BREACH INFORMATION? .....	93
6.2.7	DO YOU HAVE, IN THIS ORGANISATION, MITIGATION STRATEGIES ON INFORMATION MANAGEMENT? YES/NO.....	93
6.2.8	WHAT ARE YOUR MITIGATION PLANS IN RELATION TO INFORMATION MANAGEMENT? .....	93
6.2.9	ARE ALL STAFF MEMBERS, OTHER THAN EXECUTIVE MANAGEMENT, AWARE AND KNOWLEDGEABLE OF THE INFORMATION MANAGEMENT SECURITY POLICIES PUT IN PLACE BY THE ORGANISATION? YES/NO. ....	94
6.2.10	IF YES, WHAT IS DONE IN ORDER TO ACHIEVE THIS? IF NO, WHAT DOES THE ORGANISATION VIEW AS BEING IMPORTANT IN RELATION TO INFORMATION MANAGEMENT? .....	94
6.2.11	DO YOU HAVE PREPAREDNESS PLANS TO RESPOND TO ANY POTENTIAL RISK ON INFORMATION MANAGEMENT? YES/NO. ....	95
6.2.12	HOW ARE GOVERNMENT POLICIES AND REGULATIONS ON INFORMATION MANAGEMENT ALIGNED WITH THIS ORGANISATION'S POLICIES? .....	95
6.2.13	HOW ARE THE ORGANISATION'S TECHNOLOGY SYSTEMS ALIGNED TO THE STRATEGIC PLANS OF THE ORGANISATION IN RELATION TO INFORMATION MANAGEMENT? .....	96
6.2.14	IF IT'S NOT ALIGNED, WHY? .....	96
6.2.15	WHAT ARE THE ORGANISATION'S RISK MANAGEMENT PLANS TO DEAL WITH INFORMATION MANAGEMENT BREACHES? .....	96
6.3	SUMMARY .....	97
<b>CHAPTER SEVEN: DISCUSSION OF FINDINGS .....</b>		<b>98</b>
7.1	INTRODUCTION.....	98
7.2	BREACHING OF DATA IN A FINANCIAL INSTITUTION.....	98
7.3	INFORMATION MANAGEMENT MITIGATION IN A FINANCIAL INSTITUTION .....	99
7.4	INFORMATION MANAGEMENT PREPAREDNESS IN A FINANCIAL INSTITUTION .....	101
7.5	INFORMATION MANAGEMENT SYSTEMS IN A FINANCIAL INSTITUTION .....	102
7.6	RISK RESPONSE AND RECOVERY IN A FINANCIAL INSTITUTION .....	104
7.7	SUMMARY .....	104
<b>CHAPTER EIGHT: CONCLUSION AND RESOMENDATIONS .....</b>		<b>106</b>
8.1	INTRODUCTION.....	106



8.2	CONCLUSION .....	106
8.3	RECOMMENDATIONS FOR THE ORGANISATION.....	107
8.3.1	BREACHING OF DATA IN A FINANCIAL INSTITUTION.....	107
8.3.2	INFORMATION MANAGEMENT MITIGATION IN A FINANCIAL INSTITUTION.....	108
8.3.3	INFORMATION MANAGEMENT PREPAREDNESS IN A FINANCIAL INSTITUTION .....	108
8.3.4	INFORMATION MANAGEMENT SYSTEMS IN A FINANCIAL INSTITUTION .....	108
8.3.5	RISK RESPONSE AND RECOVERY IN A FINANCIAL INSTITUTION .....	109
8.4	LIMITATIONS OF THE STUDY .....	109
8.5	GUIDELINES FOR FUTURE RESEARCHERS.....	109
	<b>REFERENCES .....</b>	<b>110</b>
	<b>APPENDIX A: STRUCTURED QUESTIONNAIRE .....</b>	<b>118</b>
	<b>APPENDIX B: SEMI STRUCTURED IN-DEPTH INTERVIEWS .....</b>	<b>121</b>
	<b>APPENDIX C: HYPOTHESIS TESTING.....</b>	<b>162</b>
	<b>APPENDIX D: CORRELATIONS.....</b>	<b>163</b>
	<b>APPENDIX E: ROTATED COMPONENT MATRIX.....</b>	<b>164</b>
	<b>APPENDIX F: CHI-SQUARE TEST .....</b>	<b>166</b>
	<b>APPENDIX G: ETHICAL CLEARANCE .....</b>	<b>168</b>
	<b>APPENDIX H: PROFESSIONAL EDITING CERTIFICATE .....</b>	<b>169</b>
	<b>APPENDIX I: TURN IT IN CONFIRMATION .....</b>	<b>170</b>

## CHAPTER ONE: INTRODUCTION

There has been a perception in the industry that employees breach data and fail to secure their organisational personal information. Collins, Sainato and Khey (2011: 800) revealed 2219 documented data breaches from 2005 to 2010 reported by the Privacy Rights Clearinghouse. Gordon, Martin and Zhoe (2011: 33) indicate that from 2007 to 2008, information security breaches have increased by 50%. According to Fisher (2013: 217), data breaches could result in fraudulent activities taking place. The study conducted by Fisher (2013: 217) found that there were 419 reported data breaching incidents resulting in the potential exposure of over 20 million confidential records. A \$3 million fine was handed down to a health insurance company in America as a result of data breaches (KPMG, 2013). The Advocate Health Group reported in 2013 that four of its computers were stolen, and this was one of the largest Health Insurance Portability and Accountability Act of 1996 breaches ever reported (Kieke, 2014: 47).

In the financial services industry, risks are greater than ever before, and risk management has moved to the centre of defining performance. More recent risks include regulatory risks and human resource risks (Haneef, Riaz, Ramzan, Rana, Ishaq & Karim, 2012: 307). Risk management is an important aspect in business and IT governance as it is a strategy to achieve efficiency (Willenweber, Jahner & Krcmar, 2008: 1). According to Rooney and Cuganesan (2015: 133), risk strategy and management control practices are required to be examined in financial institutions with activities and controls adopted by managers to mitigate risks. Fenz, Heurix, Neubauer and Pechstein (2014: 411-412) note that an early approach to information security risk management does not distinguish between highly frequent, low impact and rare high impact events. Zhou, Vasconcelos and Nunes (2008: 166-167) explain that risk assessment is an integral process in information systems as it provides risk control in the business environment in anticipating future risk concerns.

There have been high profile data breaches in the United Kingdom of late, which has resulted in guidance and recommendations to help organisations implement and monitor policies on personal information standards (Young, 2010). Information breaches by employees occur on a regular basis and are, generally, not reported by the organisation as it is often not in the organisation's interest to do so. This, therefore, results in little being known about the conditions which led to the information breaches and further results in there being minimal useful information to predict and prevent future information breaching occurrences (Shropshire, 2009: 296). Organisations could lose consumer confidence and market share as a result of data breaches, which could, therefore, be very costly to the organisation (Garrison & Ncube, 2011: 216). Combe (2009: 395) notes that it may be considered unrealistic to expect information privacy not to be compromised to a certain extent as a result of the new technological age. According to Efraimidis, Drosatos, Nalbadis and Tasidou (2009: 311), since

the internet and technology became popular, protecting personal data is more essential than ever. In order for information to be protected, several organisations and countries have issued privacy regulations that need to be followed.

The study is informed by the views expressed above on data breaches and information management even though this study further investigates contingency plans, business processes, systems, strategies and policies and programmes surrounding information management which are discussed in more detail below.

### **1.1 Problem Statement**

There is a perception that financial institutions are weak based on the number and severity of information breaching incidents and financial institutions failing to secure personal information. Sujatha (2011: 137-138) argues that one of the main problems addressed by consumers in the banking industry is their concern about identity theft and hackers; consumers also worry about fraudulent activity and security threats. A phishing attack was launched on a leading bank in India whereby customers were asked for personal details (Gupta, 2012: 243). Based on these authors' research, information breaches and security of information is at the front-minds of consumers, and organisations in the financial industry are not completely secure when it comes to protecting customer information through their systems.

### **1.2 Research Aim and objectives**

The primary objectives of this study are as follows:

- To explore the shortfalls of information security on a South African financial institution.
- To investigate if data remains separate and privacy is ensured.
- To investigate responsiveness of business processes on information management.
- To investigate the capability of systems on information management.
- To investigate the strategies formulated for information management.
- To investigate projects and programmes aimed at addressing information management.
- To investigate contingency plans on how to respond to the financial risk in respect to information management.
- To provide recommendations based on the empirical findings.

### 1.3 Research Questions

The study was guided by the following questions:

- What are the shortfalls of information security in a selected South African financial institution?
- Are the institution's contingency plans (preparedness, mitigation, response and recovery) effective for any forthcoming risk?
- What changes does the organisation need to consider adopting as a result of information security?
- How are the various value chains of the organisation affected by information security?

### 1.4 Preliminary Literature Review

There is a growing increase in concern for information privacy by governments, businesses and consumers (Smith, Dinev & Heng, 2011: 990). According to Smith et al. (2011: 990), there is a difference between privacy and information privacy. Privacy relates to the physical access of an individual and their surroundings such as private space. Information relates to individually identifiable personal information. In today's times, information is viewed as a commodity for organisations, and without it, many organisations will not be able to operate (Van Niekerk & Van Solms, 2010: 476). For organisations, there are many risks related to information security which could result in a loss of credibility for the organisation as well as monetary damage; therefore, making sure that information is secure and safe has become one of management's top priorities (Bulgurcu, Cavusoglu & Benbasat, 2010: 524).

When customer information is breached by organisations, it has a long-term negative impact on the organisation (Malhotra & Malhotra, 2011:46). Bulgurcu et al. (2010: 524) note that in order to reduce these risks, organisations require technology-based solutions, but organisations also have to focus on individual and organisational perspectives and employees compliance with information security policies as employees can be the weak link in information security. Organisations have to protect information from the increased levels of cyber threat activities by implementing security programs and having security controls and policies in place to protect information (Knapp, Morris, Marshall & Byrd, 2009: 1). Knapp et al. (2009: 2) explain that a policy is a general rule passed by the organisation to limit the discretion of employees. Information systems is a crucial area for organisations in order to protect information, but technology is not sufficient as end-user security behaviour is gaining more attention and can also prove more difficult to monitor (Herath & Rao, 2009: 154). There should be an information security culture adopted by organisations in order to obtain the required information security (Van Niekerk & Van Solms, 2010: 477). According to Gable (2014: 39), an Information

Governance (IG) program should be adopted to protect private information which ensures that personal information is protected from the moment it is created to the time it undergoes final disposition. Kosciejew (2014: 30) adds more detail to Gable's note on IG by stating that governments or regulators should impose auditing requirements on organisations who use personal information and that any application that looks at personal information should be inspected. Based on these authors' arguments, there is a clear increase on the focus of personal information by organisations and having the necessary policies and structures in place to ensure that information is secure not only from a technology and system perspective but also by having employees comply and understand what is required from them. Literature also makes reference to the negative impacts of information breaches by an organisation with clear reference to how this negative impact can decrease the monetary position of organisations and ultimately, its sustainability. This could, therefore, cause organisations to shut their doors.

There have been significant regulatory changes passed to guide corporate governance, particularly in emerging economies (Siddiqui, 2009: 253). The King I Report on corporate governance was introduced in South Africa in 1994 with ethical aspects and organisations adopting good ethical and environmental practises being one of the areas addressed (Ehlers & Lazenby, 2010: 96). According to Ehlers and Lazenby (2010), the third draft of the King Report, King III, was drafted in 2009 and explains that the King Report on corporate governance is the conclusive law on corporate governance in South Africa. The King reports are stakeholder-orientated and draw attention to the need for organisations to act in a responsible manner towards all its stakeholders (Brennan and Solomon, 2008: 11). According to Malhotra and Malhotra's (2011: 45) research, consumers are concerned about the information collected on them and how it is being used and protected by organisations. More recently, governments world-wide have adopted access to information laws with the main reasons being attributed to global media growth, the technology boom, and national security issues (Relly & Sabharwal, 2008: 148). The Protection of Personal Information (POPI) Act was promulgated on 26 November 2013 by the South African government. POPI focuses on protecting the flow of information and advancing the right of access to information; if any organisation processes personal data, then it needs to be done in compliance with the POPI Act (South Africa, 2013: 34). The POPI Act can be regarded as one of the broadest privacy legislation in the world and its requirements make it difficult to fully understand the implications of the Act (Burmeister, 2014: 7). Based on the increase in consumer awareness on how their information is used and protected by organisations as well as other factors such as technology advancements, as stated by the authors, governments have specific laws and regulations for organisations to abide by pertaining to customer information.

## **1.5 Research outline**

### **Chapter 1: Background and Scope**

This chapter commences by providing the background of the study and an introduction to what sparked the research and the views of various authors on information management. The problem statement and the purpose of the study are briefly discussed. This chapter also covers the research questions and objectives of the study. This is followed by the literature review, conceptual framework and chapter inventory.

### **Chapter 2 and 3: Literature Review**

This chapter is split into 2 sub-chapters namely; International perspective and the South African context. This chapter includes an in-depth review of the international perspective of information management, including how different countries' views on information management. A comparison on the views, similarities and differences of information management, as seen by developed and developing countries, is made as well as an in-depth review of information management by South African organisations and government.

### **Chapter 4: Research Methodology**

This research is exploratory in nature with an empirical investigation. The research approach is both quantitative and qualitative. Structured questionnaires and in-depth interviews are the instruments used to collect data. Reliability and validity testing is also reported as taking place in order to test the applicability, consistency and neutrality.

### **Chapter 5 and 6: Data presentation and analysis of results**

In this chapter the research data is analysed. The data collected and the statistical analysis of the data are presented. The presentation of the data includes graphs and tabulation. The quantitative and qualitative results are split over 2 chapters.

### **Chapter 7: Discussion of findings**

From the data collected and analysis done on the data, the findings of the research study are presented. The results of the framework focus on, but not limited to, business process, strategies, systems and programmes on information management.

### **Chapter 8: Conclusion and Recommendations**

This chapter is split into 3 sub sections namely: recommendations for the organisation, guidelines for future researchers and limitations to the study. In this chapter, conclusions and recommendations are

drawn from the discussed findings. This includes recommendations for the organisation to adopt based on the outcome of the findings. A guideline for future researchers who wish to investigate the subject of information management is covered as well as an explanation of limitations experienced whilst conducting the study.

## **CHAPTER TWO: INFORMATION MANAGEMENT IN A FINANCIAL INSTITUTION: AN INTERNATIONAL INSTITUTION**

### **2.1 Introduction**

This chapter reviews literature on various aspects of information management from an international perspective and how factors of information are viewed abroad. It consists of sub-sections which critically review information privacy, information security systems, data breaches, security programmes, employee behaviour relating to information management and security, information risk assessment and management, handling information and information governance outsourcing.

### **2.2 Information privacy**

There is a growing increase in concern for information privacy by governments, business and consumers. There is a difference between privacy and information privacy (Smith, Dinev & Heng, 2011: 990). Privacy relates to the physical access of an individual and their surroundings such as private space whilst information relates to individually identifiable personal information. Nowadays, information is viewed as a commodity for organisations, and without it, many organisations will not be able to operate (Van Niekerk & Van Solms, 2010: 476). For organisations, there are many risks related to information security which could result in a loss of creditability for the organisation as well as monetary damage; therefore, making sure that information is secure and safe has become one of management's top priorities (Bulgurcu, Cavusoglu & Benbasat, 2010: 524). When customer information is breached by organisations, it has a long-term negative impact on the organisation (Malhotra & Malhotra, 2011:46).

Bulgurcu et al. (2010: 524) note that in order to reduce these risks, organisations require technology-based solutions, but organisations also have to focus on individual and organisational perspectives and employees compliance with information security policies as employees can be the weak link in information security. Organisations have to protect information from the increased levels of cyber threat activities by implementing security programs and having security controls and policies in place to protect information (Knapp, Morris, Marshall & Byrd, 2009: 1).

Knapp et al. (2009: 2) explain that a policy is a general rule passed by the organisation to limit the discretion of employees. Information systems is a crucial area for organisations in order to protect information, but technology is not sufficient as end-user security behaviour is gaining more attention and can also prove more difficult to monitor (Herath & Rao, 2009: 154). There should be an information security culture adopted by organisations in order to obtain the required information security (Van Niekerk & Van Solms, 2010: 477). According to Gable (2014: 39), an Information



Governance (IG) program should be adopted to protect private information which ensures that personal information is protected from the moment it is created to the time it undergoes final disposition. Kosciejew (2014: 30) adds more detail to Gable's note on IG by stating that governments or regulators should impose auditing requirements on organisations who use personal information and that any application that looks at personal information should be inspected.

Based on these authors' arguments, there is a clear increase on the focus of personal information by organisations and having the necessary policies and structures in place to ensure that information is secure not only from a technology and system perspective but also by having employees comply and understand what is required from them. Literature also makes reference to the negative impacts of information breaches by an organisation with clear reference to how this negative impact can decrease the monetary position of organisations and ultimately, its sustainability. This could, therefore, cause organisations to shut their doors. These perspectives presented are significant to this study as information privacy and security is a key factor surrounding information management. Part of what this study reviewed and analysed breaching of data in a selected financial institution as well as looked into employees' alignment to policies within the organisation relating to information management and whether information is kept separate and secure in the organisation.

### **2.3 Information security systems**

There is a world-wide trend to adopt and implement information communication technology systems in order to gain efficiency in the way that the organisation operates. The implementation of technology can be attributed to the natural progression of organisations changing and organisations looking to improve strategic and technological tactics. An important aspect of technology adoption by organisations, however, is also determined by the size and epidemic effect of the organisation. As the implementation of information systems can come at a big financial cost, policymakers should act as an advisory regarding the establishment of information systems by looking at the main determinants and patterns of information systems to design corporate and policy strategies for the successful deployment thereof (Choi, Kim, Jun & Kim, 2011: 1466-1476). The concept of information security risk assessment can quantify risk management through the analysis of the threats of various networks and systems through various approaches and tools. Some of these methods include qualitative, quantitative methods as well as a combination of the two methods. Organisations need to select appropriate and effective measures to fight information security threats in an active manner as this is a vital aspect to solve the problem of information system security. Information risk assessment is, however, a complex process which, at times, is a real-time process (Chen, Pedrycz, Ma & Wang, 2014: 687).

According to Tsohou, Kokolakis, Lambrinouidakis and Gritzalis (2010: 351-352), there should be standardisation of information security systems as this will provide conformity assessment mechanisms to ensure that it meets internationally accepted rules and practises. In the UK, organisations are more regularly expected to demonstrate to customers how compliant they are in terms of the information security and standard guidelines. There are still, however, many UK organisations that are not aware of the guidelines. Organisations could enhance their awareness of security standards through a four-layered framework that links existing security standards systematically and provides security management guidelines. This framework includes the planning phase which consists of guidelines to risk assessment; the second phase consists of the implementation of a risk treatment plan; the third consists of monitoring and auditing and the fourth phase consist of action where corrective actions can take place.

It is noted that the success of this is only really seen if all four phases are implemented. Gal and Berente (2008: 133-150) add that implementing information systems is a complex process whereby all stakeholder groups have to be involved as their needs and requirements are different as well as their understanding or perception of the technology which may be different. People's interpretation of the purpose of the technology may vary and therefore, it is also of importance to involve all stakeholders. These interpretations could then have a substantial impact on the success of the implementation of the information systems. The implementation of information systems cannot only be looked at from a technological perspective or framework as social representations also have to be addressed.

Social representations could give a more fundamental approach to information system implementation. This social representations theory includes shaping the organisational members' perceptions of the technology thereby affecting the success of the implementation of these technologies. These social representations help organisations and groups in the organisation to understand the meaningfulness of information systems. According to Nazimoglu and Ozsen (2010: 351), the adoption of information technology can have a positive or negative effect on perceptions and behaviours; consequently, technology should be adopted in a way which is acceptable to individuals and customers but also in a way that services the organisation. Moghavvemi and Salleh (2014: 614) note that "performance expectancy and the propensity to act are determinants of behavioural intention to adopt and use information systems by entrepreneurs".

The authors propose that even in this technology age and the rapid expansion of information technologies being adopted by organisations, the organisation should not just jump in blindly to implement these technologies but should rather assess the needs, size and prevalence of the

organisation when looking to implement information technology systems. This, therefore, forms part of the overall strategic policy and plan of the organisation. It is clearly stated that implementing information technology and information security cannot just be done from a technical perspective but should involve a social aspect as well whereby all stakeholders need to be involved. This shapes the organisation's members and allows for meaningful implementation of information technology. When looking at the information security risks to the organisation, it is mentioned that organisations can assess risk threats by using various tools and methods available while in certain studies, organisations were requested to demonstrate how effective and compliant their information security mechanisms are. This study reviewed and analysed respondents' attitudes towards information technology based solutions within an organisation as well as the respondents' views on protection and security that comes with having information technology system solutions at the related organisation. It is noted in the literature that data breaches is an information security risk. Data breaches in relation to technology systems as well employees are discussed in the next section.

#### **2.4 Data breaches: Technology vs. Employee**

Information systems is a cornerstone for any organisation if they want to survive and compete with global fierce competition. With the rising number in security risk incidents, information systems are becoming more exposed to risk and breaches (Al-Mukahal & Alshare, 2015: 102-103). In order to gain a competitive advantage, organisations need to know how to analyse and manage information technology risks as information technology has become the backbone of commerce (Nazimoglu & Ozsen, 2010: 351). The use of information technology is considered as the common denominator for the competitiveness of an organisation (Moghavvemi & Salleh, 2014: 600). As a result of data breaches, organisations also spend money to prevent future breaches and loss of revenue.

It is of importance that organisational policies are in place to quickly respond to data breaches (Garrison & Ncube, 2011: 216-217). Katos and Patel (2008: 78) argue that the demand for privacy security technology depends on the level of security required whereby the higher the level of privacy information needed, the more security systems may be demanded. With the need for technology on the rise and the need to secure these technologies from breaches, Al-Mukahal and Alshare (2015: 103-115) mention that employees also breach data and that the reason for employees violating or not violating security policies when it comes to information management could vary from: deterrence, neutralisation, rational choice theories to habit, protection motivation and planned behaviour of individuals. Deterrence consists of behaviours whereby individuals will choose crime only when it pays off but are less likely to commit crime when the penalties against the crime are harsher. Neutralisation focuses on people's moral obligation to abide by laws while planned behaviour refers to individuals committing to an action if they have planned to do it before committing it. In developing

countries, it was found that trust is a significant factor in predicting whether information security policy will be breached. Another substantial factor in developing countries is that the clarity of the scope of the information security policy can predict if violations will occur while uncertainty and avoidance can moderate the relationship between the mentioned trust and policy scope in relation to the impact of information security violations. D'Arcy and Green (2014: 484) state that it has been found that security related and general working environment factors could contribute to an employee's security compliance while an employee's position, the industry in which the organisation operates and the amount of time that an employee has been employed at the organisation also play a role in employee security compliance.

The perspective of the authors are that information systems are critical to the survival of an organisation with the concept of analysing information systems coming through once more. Data breaches are said to be topical issue on information systems whereby organisations need to invest in prevention of data breaches and securing information. It is highlighted that employees' knowledge and awareness of information security is a key area that needs to be assessed to prevent or minimise data breaches as there are various factors that could be looked at to determine the likelihood and extent to which employees violate information security policies and procedures. This study evaluated respondents' perceptions of data breaches as well as the likelihood of respondents across the value chain of the organisation breaching organisational personal information. Incidents of data breaches and mitigation programmes are covered in the following section.

## **2.5 Data breaching incidents and security programmes**

According to Pike (2009: 16-17), in the United States (US), there are over 40 states that passed legislation which required organisations to provide notification of data breaches. Katos and Patel (2008: 75) note that privacy could be considered to be a right that people should have, yet security has shown an attempt to surrender the right to privacy. Holtfreter and Harrington (2015: 242-259) confirm that in 2012, a US organisation was a victim of data breaches whereby hackers gained access to customers' personal information. These data breaches occur when individuals' personal information like bank account numbers, passwords and email addresses, for example, are accessed for the purpose of fraudulent activities. There have been thousands of data breaches that occurred in the US over the past seven years across various industries while the numbers are increasing at a rapid rate. A record of these data breaches across different industries are mentioned whereby in 2005, the Bank of America lost computer tapes of 1.2 million customers with social security and bank account numbers on it. In 2008, New York Harley-Davidson reported that a laptop was missing with 60000 Harley Owners Group members' names, credit card numbers and addresses on it. In the non-profit industry, in 2006, an employee of the American Red Cross got access to 1 million records which

included donor social security numbers by intruding the organisations database. Data breaches can, therefore, occur from internal or external sources, which could compromise millions of records.

Singh, Gupta and Ojha (2014: 644) state that the increased dependency on information and information assets has resulted in information security being a great need to an organisation. Advancements in technology have posed a threat to business information with high level technological solutions proposed and implemented to protect information; however, information security still remains a challenge in organisations due to not addressing information security at a strategic level within the organisation. It is said that information security is not a technological issue but also a management issue, and behavioural aspects need to be considered when addressing the concept of information management. The four waves to information security are: technology, management, institutional and governance. Information systems management can no longer be seen to only be an IT issue and one that needs to be handled by the IT department. It has to be a collective responsibility within the organisation with key management factors highlighted in information security. According to Abu-Musa (2012: 236), a comprehensive security programme includes:

- Development and maintenance of security policies;
- Assignment of roles, responsibilities, authority and accountability;
- Development and maintenance of a security and control framework that consists of standards, measures, practices, and procedures;
- Periodic assessments of risks and business impact analyses;
- Classification and assignment of ownership of information assets;
- Adequate, effective, and tested controls for people, processes, and technology;
- Integration of security into all organizational processes;
- Processes to monitor security elements;
- Information security incident management;
- Effective identity and access management processes for users and suppliers of information;
- Meaningful monitoring and metrics of security performance;
- Education of all users, managers, and board members regarding information security requirements;
- Annual information security evaluations and performance reports to the board of directors;
- Plans for remedial action to address information security deficiencies;
- Training in the operation of security processes; and
- Development and testing of plans for continuing the business in case of interruption or disaster.

The authors make reference to a number of data breaching incidents experienced by organisations. These incidents range across industries, including non-profit organisations. The view that the advancement of technology is a threat to individuals comes through here while also advising that the behaviour of management needs to be assessed in information security. Here again, it is advised that there are various stakeholders that need to be involved in information security and clarifying that it is not an IT only issue. This study evaluates respondents' views on what the employees' link is to information security and how important the employee is in ensuring information is kept private. In addition, this study also looks at respondents' training received in information security and investigates if there are projects and programmes aimed at addressing information management. Risks and reasons for employees breaching data or security policies are discussed further in the following section.

## **2.6 Employee behaviour relating to information management and security**

Through knowledge management, as a discipline, managers could increase their security knowledge that is needed in information security while it could also be beneficial to the organisation to examine the relationship between management awareness and actions versus general employee awareness of information security (Garrison & Ncube, 2011: 217). Katos and Patel (2008: 82) add that security and privacy studies should be done through cross-methodology while looking at the macro-environment. According to Thompson and Van Niekerk (2012: 39-43), employees can often be the weakest link when it comes to safe guarding information security. This is likely due to an unconcern of information security as individual employees may not feel that it is their responsibility to protect this information. Organisations, therefore, need to adopt a culture whereby information security forms part of the organisational culture and influence employees' behaviour towards information security. This will not, however, eliminate information security issues but will reduce these.

Organisations firstly need to set goals and have organisational behaviour form part of these goals. The clearly defined goals lead to better performance of employees as the goals are not vague, and employees' performance can be measured against the goals. Through encouraging prosocial behaviour, employees' behaviour will be to promote and protect the organisation when looking at it in the context of the organisation and information security. Hagen and Albrechtsen (2009: 388-405) argues that commitment is required from employees at all levels of the organisation in order to ensure that information security is maintained and that employee compliance is best achieved through awareness campaigns and education. Training and educating employees is more effective than formal procedures and controls put in place by the organisation, but many organisations do not provide adequate training to employees in relation to information security. A simple and common way to evaluate if information security training is working is to conduct quizzes as well as before-and-after

surveys. Information security awareness programmes conducted at a leading maritime organisation in Europe indicated that there was a significant increase in the behaviour of employees in relation to information security. Frangopoulos, Eloff and Venter (2013: 54) are of the view that psychological risk mitigation management should be done in all disciplines of management studies as psychological risks affects information security.

Hagmann (2013: 228-230) states that information governance could be seen as a decision about information and information management; however, organisations develop their own definition and understanding of information governance depending on their needs and priorities. IT governance and information governance has not really been separated by many organisations. Specialists in the field of enterprise information management seem to embrace the value of information governance to organisations, but there are only a few who actually do anything about it. There is a gap between what individuals are aspiring to do and what is being implemented in reality. Executive members of the organisation should support the potential synergies that an information governance programme offers, and the biggest challenge to unified governance is understanding that all areas of the business need to be involved to achieve the business goals.

Ko and Fink (2010: 662-663) add that information technology governance is an integral part of corporate governance and requires senior management to provide the necessary direction. One view of information technology governance is the architectural view which looks at it from an organisational capacity angle which is run by executive management. Kahraman, Kaya and Cevikcan (2011: 360-375) note that enterprise information management systems are adopted by many organisations for the purpose of administration, control, reporting and transaction management. The key is to integrate cross-functional business areas and integrate business processes and information, which will ultimately increase profit and market share. Management can use the information from the enterprise information management system as decision-making is one of the most important tasks for managers. The management of information in organisations is constantly a topical subject while evaluating its efficiency is a critical task. Otapah and Dadzie (2013: 144) argue that organisations are setting up information units which allows for specific information to be available for the right business unit in order to aid these business units to make the correct decisions. This aims at having the right information available to users without the clutter of unnecessary information for users. By doing this, it allows the organisation to accomplish its strategic objectives. Caldwell (2008: 163-166) adds that knowledge management ensures that the correct information is supplied to the right people when needed. The author further argues that this ensures that proactive rather than reactive decisions are made and maximizes the return on value from information.

As authors make reference to organisations setting up business units in relation to information units and having certain information available to the appropriate employee, Zhang, Reithel and Li (2009: 330-338) note that an effective technical security protection and trained employees are important security counter-measures to breaching information in an organisation Frangopoulos et al. (2013: 53-61) add that major issues in information management systems can be caused by the human, that is, the employee or the end user. Technical measures which strengthen information security do not help when users are compromised. Breaches could occur deliberately or accidentally as a result of employee negligence. Employees are, therefore, humans with their own shortcomings and cannot be looked at within the bulk information security point of view. When psychological risks identification management and information security are combined, there may be a better understanding as to the reason for information security failing when there are specific controls and measures in place that deal with information security.

D'Arcy and Green (2014: 474) state that to encourage employees to comply with authorised information security policies is a great challenge for organisations. Employees may, at times, rush work to increase productivity and in the process, consciously violate certain authorised procedures, guidelines and information security policies. Employees may even, at times, violate these mentioned areas with the purpose of harmful intentions such as stealing organisational information or sabotaging the organisation. Lacey (2010: 12) adds that an approach is required to the business environment which is less focused and constrained by process but rather implementing security which pays attention to people. To achieve this, organisations need to shift the emphasis towards people, relationships and information flows.

Based on the author's perspective, it is valuable to adopt knowledge management whereby managers could assess their awareness and actions in conjunction with that of employees in relation to information security. The area of employees possibly being a weak link in information security comes through strongly, and it is proposed by these authors that information security needs to form part of the organisation's culture in order to influence employee behaviour. Commitment from all staff levels is required in order to succeed, and training and information sessions could be seen as more valuable than just putting policies in place for employees to abide by. Executive members, being heavily involved in information security and IT governance, come through strongly. Ensuring that there are cross-functional synergies from the various business units is highlighted while the opinion differs from other authors stating that specific information should be passed to specific business units only to avoid information clutter as this can be seen as part of knowledge management which ensures proactive decision-making. This relates closely to the study of information management systems in how the requirements for these systems are analysed and the output design of data is developed by



IT in terms of which data is available to various departments or individuals. Identifying information security risks and management thereof is covered in the next section. The human element of breaching information is common across the majority of the authors, and it is noted that this should be addressed by organisations through understanding the variables and causes of employees' breaching of information. This study examined senior management plans and efforts to ensure that employees are trained on information management and analysed whether there are information management awareness programmes initiated by senior management.

## **2.7 Information risk assessment and management**

By analysing data breaching risks, organisations could lower security budgets by implementing information security policies (Garrison & Ncube, 2011: 228). It has previously been the perception that information systems were costly, took long to develop and that the benefits of these information systems did not deliver what they were intended to deliver. Risk management often focuses on managing and controlling security breaches, individual behaviour and compliance breaches. Before risks can be managed, the risks need to be identified. Risk management is a structured approach which manages uncertainty through risk assessments, strategies and risk mitigations and handles the effects of risks and reduces the negative effects of these risks (Nazimoglu & Ozsen, 2010: 351). Risk assessments often look at information as objects that can be threatened and requires protection. Information is, however, also strategic value of tacit and explicit organisational knowledge which has a competitive and commercial value as it could affect an organisations' ability to operate. Protection of knowledge has not received the level of attention that it should in organisations (Shedden, Scheepers, Smith & Ahmad 2011: 152-153).

Organisations need to ensure that information is adequately secured as information security has become an important part of daily operations. Well planned security policies should be set by organisations and security awareness, and education should be implemented in relation to information security. This information security should involve the necessary risk management and should not just be seen as a technical issue. Active involvement of executives is required when tackling this issue whereby they need to assess the threats to the organisation and develop contingencies and responses to the threats (Abu-Musa, 2012:226-227). Certain organisations may take into account information security when doing their financial budgeting, but the effectiveness of the spending can affect the organisation, stakeholders and customers a great deal. This budgeting process is an iterative process whereby organisations evaluate information security spending by considering whether they should spend, how much they should spend and lastly, what they should buy. Approaches exist to determine the right amount of money to spend on information security; however, what is important is to determine the extent to which the information security adds value to the

organisation. This could be tough to determine though as once implemented, if there are no breaches, it is hard to know whether it is a result of information security or if there would not be any breaches even without the information security being in place (Stewart, 2012: 312-313). Information security breaches can decrease employee productivity but also affect an organisation's reputation by damaging customer confidence in the organisation and negatively impacting the economic condition of the organisation (Zhang, Reithel & Li, 2009: 330-338).

Based on these authors' perspectives, risk assessment is key in information systems whereby risks must be identified in order to manage them. This then handles the effects of risks and reduces negative impacts that it may have. Risk management should involve various stakeholders within the organisation, and threats against information should be assessed with the appropriate contingencies put in place. Information security does not always get the necessary focus that it should get, and organisations should efficiently plan for this in their budgeting process because even though it is difficult to measure the success of information security, it is still of utmost importance to ensure that security measures are in place. This study reviews preparedness plans and risk recovery plans as one area of analysis was to evaluate the level and preparedness and response to information risks. The handling of information by employees within the organisation is discussed in the next section.

## **2.8 Handling Information**

In business today, information privacy laws and regulations are strict pertaining to how customer information is protected. It seems that every industry and economy is affected by privacy legislation that is emerging. Similar laws in Europe and Asia are emerging as those to the US such as the Fair Credit Reporting Act (Johnston & Warkentin, 2008: 5-6). When generating electronic information, there are ethical considerations and implications. These functions of electronic information include originating, processing, storing and distributing the information. There is a responsibility on those individuals and organisations who perform these tasks. There is a great deal of focus on employee practises as this could have legal concerns associated to it. There is, however, less scrutiny on the methods used to collect data even though there are ethical considerations that are related to this. Ethical practices in electronic information impacts the entire organisation while information systems also have an ethical element to it. Organisations who invest in ethics could, in turn, find substantial rewards in employee morale and performance (Desai & Von de Embse, 2008: 20-26). From an information security perspective, ethics are not covered to the same degree as risk, policy and strategy (Ahmad & Maynard, 2014: 529).

In recent times, the process of personal information management has been promoted and divided into three main areas. The first area looks at the features and problems with software as well as

evaluating and comparing various software. The second area looking at how information is gathered and managed for future use. The third are initiatives by information professionals to provide training and support. Personal information management is a process and study of the activities that are performed when creating, storing, maintaining, retrieving, using and distributing information. These are also related to the software and personal databases. Information practices could be shaped by certain social and cultural factors while studies should be concentrating more on how to create a personal information management culture within organisations (Fourie, 2011: 387-389).

There are a number of personal information management tools that exist which cater for managing documents in electronic formats (Otapah & Dadzie, 2013: 144). Lacey (2010: 7) makes mention that security culture in organisations could mean different things to different people, and organisations have not yet defined precisely what security culture actually entails. For certain individuals, this involves setting up and applying security controls while for others, it is about having a mind-set of being cautious and suspicious. According to D'Arcy and Green (2014: 476), there are numerous concepts that are related to security culture within organisations; however, a consensus is made on three focal dimensions of security culture. These are top management commitment to security, security communication and computer monitoring. Ahmad and Maynard (2014: 513) state that managing information security in organisations is complex as it requires formal, informal and technical controls. Information managers also need to have knowledge of how security supports business objectives as well as an understanding of various security practices.

From the authors' statements, the manner in which customer information is protected is looked at in various countries and within industries with similar information privacy laws being adopted by Europe and Asia as is in North America. There is a responsibility upon organisations who consume customer information; however, it is mentioned that there is less scrutiny on how the information is collected. The responsibility on organisations also involves an ethical point of view while these ethical elements are not covered with same level of vigour as that of information risks, policies and procedures. Security culture comes through the literature once more, with the authors' perspective that organisations have not yet fully come to grips with what security culture really entails as it possesses various elements to it. Part of this study analyses whether information is protected by the employee and organisation from the moment the information enters the organisation and if it is handled within government and company policy. The governance of information ties in with information risks, policies and culture as information governance could provide the skeletal framework to information management within organisations. Information governance and trends are discussed in the following section.

## **2.9 International legislation on information management**

There is an increase in governments using information and communication technologies to deliver government information and services. There is also information about citizens exchanged between government departments, and this raises a concern on private and sensitive information held by governments. In New Zealand, the use of personal information by government departments is controlled by Government Acts. This also includes exchanging data about individuals with the consent of these individuals (Cullen, 2009: 405-406). Malmir and Malmir (2015: 98) argue that in today's world, the relationship between governments and citizens requires developing social and economic interactions to interfere in the private lives of people even though this was formerly seen as people's right to privacy.

According to Desai, Desai and Phelps (2012: 222-227), in the United States under the Obama administration, John Kerry is looking to draft a privacy bill of rights legislation to protect consumers' privacy. This partly stemmed from the fact that web sellers are not currently required by law to maintain the privacy of people who use their websites. There is a fear of personal consumer information being hacked even though big online retailers such as Amazon publish a privacy policy. The United States is mainly self-regulated when it comes to the use of cookies relating to online activity, but the Federal Trade Commission does not take measures or action against organisations who do not abide by their own organisational privacy policies given to users of their websites. Jianping and Zhongwei (2009: 229) argues that in the United States, financial privacy protection is a relative complete legislation system while keeping a balance between public power and private right.

According to Sumanjeet (2010: 274), in India, the Information Technology Act of 2000 and amendments in 2008 are aimed at providing a legal framework for e-commerce and cyber activity. This Act was initially passed to regulate activities relating to e-commerce, cyber offences and e-governance. Pope and Lowen (2009: 301-305) state that there are subtle differences in the concept of consumer privacy in the USA versus other countries and that cultural reasons and governmental policies towards privacy protections could be influential factors that result in the differences. When organisations do multinational marketing campaigns, different regulations and cultural factors should be taken into account as privacy issues are a major concern for consumers and the news media. While consumers' perceptions of privacy have become more important to organisations' marketing function, there are many people who are unclear as to what their rights are when it comes to privacy of information. It has become more relevant for marketers to segment consumers and take into account international privacy laws and attitudes as the legal framework dictates if and how an organisation can transfer information across borders.

It was found that the differences in attitudes between Japanese and American consumers towards telemarketing, direct marketing and government regulations are partly determined by the differences in culture. In the USA, private consumer information is taken on a more voluntary approach while in neighbouring Canada, it is driven by federal regulation. Collin (2009: 395-399) adds that in parts of Europe, the European Union Data Protection Directive is in effect and aims to protect privacy when it comes to processing and moving personal data whereby data subjects can object to having their personal data processed. The UK government has instilled the Data Protection Act (1995) with the key determinant being fair and lawful gathering and processing of data by organisations as well as consent and data sharing laws.

The Act, however, offers specific guidance, so whether organisations are compliant or not depends on adherence to the Information Commissioners guidance. Murata and Orito (2008: 234) state that in Japan, the Act on the Protection of Personal Information (APPI) went into effect 1 April 2005 but has not performed well in enhancing handling of personal information as the Act has caused more confusion about handling personal information in Japans society. One of the key missing aspects is that the APPI fails to adapt to the modern information society. According to Jianping and Zhongwei (2009: 229), in China, the first time privacy law was provided was in January 2006 where there is a section about human rights in the Civil Code; this states that a natural person should enjoy the right to privacy. Privacy law in China remains at the beginning stages of researching and drafting.

The authors make reference to laws and governance being different across countries whereby there are countries where there is a relative complete legislation on information privacy while other countries' governments are in the early stages of adopting and drafting these information protection and privacy laws. The US and UK have instilled specific laws on this and are continuing to look at new technological factors influencing laws such as reviewing how online stores protects consumer information. In this study, senior managers are interviewed in order to understand and analyse how government legislation impacts the organisation as well identify the challenges and opportunities brought by these governmental policies. These policies and procedures are not only applicable to staff members of the organisation but also third parties and vendors that are linked to organisation in study. The following section reviews information governance outsourcing.

## **2.10 Information governance outsourcing**

Policies, technical controls and standards have usually been the main focus of intra-organisational research on information security; however, there should also be a focus on any resilience of sub-contractors when it comes to implementing standards of information security. There is a need for organisations who use IT vendors to bargain and negotiate between vendors in order to protect the

organisations value and reputation (Jarvelainen, 2012: 333). Good security measures can improve the reputation of an organisation and give consumers the trust that they are looking for as this also avoids wasting time and money from recovering from a security incident. Effective information security governance, however, requires continuous improvement as protecting critical information should be seen as one of the main management strategies in organisations. It has been found that information security governance is an important component to the success of the organisations' overall strategy and investment; in these, information security governance has created value for organisations in Saudi Arabia. There are still, however, large numbers of cases where organisations in Saudi Arabia have no information security strategy, and management has not put formal policies on information security in place (Abu-Musa, 2012:227-269).

It has become the phenomenon of late to outsource information systems and information technology. European organisations have increased the amount of money spent on outsourcing. Organisations are driven by forces in the market to outsource certain streams of the organisation, and many do this except for the core elements of their business. Outsourcing can make it easier for the business to focus on the basic competencies of the organisation. There is also an increase in flexibility that comes with outsourcing as it could prevent the organisation from becoming technologically obsolete as well as increase the quality delivered by information systems services while having high quality IT services at the organisation's disposal. It sometimes also seems that IT is difficult to manage and outsourcing this function can minimise work that could be seen as problematic. Outsourcing, therefore, allows for a more specialised IT management. There are also risks associated with outsourcing which include the service provider not performing tasks as expected, which can be seen as a lack of compliance. When deciding to outsource, organisations need to bear in mind that with services being outsourced, organisations could lose the understanding of the service over time as the intellectual property now sits with the service provider. In Spain, large organisations consider that outsourcing provides the opportunity to achieve better technological improvements (Gonzalez, Gasco & Llopis, 2010: 284-299). In information governance, there needs to be a risk intelligence strategy that deals with both regulatory risks and business pressures. When it comes to regulatory risks, the quicker documents can be provided to auditors or regulators, the less money is spent on labour to find those documents or information. Business pressures require information to be provided quickly and easily in order for critical business decisions to be made. Organisations can implement a risk intelligence strategy by establishing a centralised information management function, providing the appropriate operation support, assigning a specific employee to be accountable for information risk management, designating implementing and maintaining controls for information risk mitigation and focusing information risk management on the categories of business risks, regulatory risks and legal discovery risks (Caldwell, 2008:163-166).

Based on these authors, good security measures can positively influence the reputation of an organisation while when outsourcing IT and information security to vendors, organisations should carefully select the vendor to use as this can impact the organisation's reputation. Many organisations have opted to outsource information security and the general IT related business stream in order to get the best quality service. It is, however, also mentioned that there are risks associated with outsourcing. Organisations should have an information security strategy which provides appropriate support to the business and its various business streams. It is also noted that some organisations have no information security strategy in place. Part of this study reviews the organisational plans to ensure that key stakeholders to the organisation such as vendors do not breach information.

## **2.11 Summary**

Literature indicates that there are different aspects to information management within organisations. Technologically based information systems are noted as important whereby organisational and customer information can be captured, stored and made available for future use. It is mentioned that information systems are key to an organisation's survival and competitive advantage. Government regulations and laws on data, privacy and personal information are a big factor for organisations as organisations are required to put in place company policies and procedures to adhere to these government laws. It is noted in literature that governments all over the world are adopting data and information privacy regulations. The theme of employees' understanding organisational policies on information security and the fact that employees could be seen as the weakest link to information security comes through strongly in the literature. Employee compliance is an area that also adds significant focus in the context of information management as it is stated that there are various factors that could determine the likelihood to which employees could infringe on information security policies and procedures, whether intentionally or unintentionally. The advancements of technology being a threat and not only an enabler to organisations and consumers is noted as it is stated that the innovations of technology have come with an increase in the number of data breaching incidents. Data breaches are said to be on the rise and affect various business sectors as well as non-profit organisations. The literature makes mention of that fact that information security within organisations does not get the necessary attention that it should and that various stakeholders across the business, not only IT, should be involved in information management and information security. Getting various areas of the organisation involved in information security ties in with literature on getting employees knowledgeable on information security and company policies relating to information management as it is stated that organisations should create a culture of information management. Breaching customer data and not having good information security measures in place could affect an organisation's reputation negatively and ultimately result in the organisation having to close down. The following chapter focuses on information management from a South African perspective. It also covers South

African legislation pertaining to information privacy and information management as well as review organisational policies and procedures on information management at a South African financial institution.



## **CHAPTER THREE: INFORMATION MANAGEMENT IN A FINANCIAL INSTITUTION: A SOUTH AFRICAN INSTITUTION**

### **3.1 Introduction**

This chapter reviews literature on various aspects of information management from a South African perspective. It consists of sub-sections which critically review corporate governance, the legislative framework on information management, the information structure and use in South African organisations and reviews information management policies at a selected South African financial institution.

### **3.2 Corporate governance**

There have been significant regulatory changes passed to guide corporate governance, particularly in emerging economies (Siddiqui, 2009: 253). The King I Report on corporate governance was introduced in South Africa in 1994 with ethical aspects and organisations adopting good ethical and environmental practises being one of the areas addressed (Ehlers & Lazenby, 2010: 96). The working definition of the 1994 King I Report on corporate governance focused on systems which organisations are controlled and directed and whereby the responsibility of publicly owned organisations lies with its board members and directors (Rossouw, van der Watt & Malan, 2002: 289). In 2002, the King II Report on corporate governance was introduced and focused on organisations moving away from the single bottom line or profit and adopting a triple bottom line approach which takes into account economic, environmental and social aspects of an organisation's activities (Cliffe Dekker Attorneys, 2002: 2).

King II was the framework for South African organisations to include environmental and social governance in their reporting (Atkins & Maroun, 2015: 199). According to Ehlers and Lazenby (2010), the third draft of the King Report, King III, was drafted in 2009 and explains that the King Report on corporate governance is the conclusive law on corporate governance in South Africa. The King reports are stakeholder-orientated and draw attention to the need for organisations to act in a responsible manner towards all its stakeholders (Brennan and Solomon, 2008: 11). Organisations in developed and developing countries face different demands and, therefore, require different structures whereby developing countries require a corporate governance framework that attracts international investment to enhance economic growth (West, 2009: 10). In order to make the most of benefits that may come with organisation's positive corporate social responsibility status, there is a risk that immoral organisations may be tempted to falsify their corporate social responsibility acts. This could be done by selectively disclosing corporate social responsibility information and, therefore, organisations

disclosing their corporate social responsibility may not necessarily be good corporates to the environment in which it operates but could, at times, look to merely favourably influence the perception of stakeholders.

The King III code of governance looks to heighten stakeholder accountability transparency of non-financial related items such as corporate social responsibility (Ackers & Eccles, 2015: 516). Organisations should get independent assurance on their sustainability reporting and external assurance providers should provide a report that organisations should also include in their sustainability reporting submissions which should describe the work performed in order to increase the reliability as well as credibility of an organisations sustainability reports (Marx & van Dyk, 2011: 49). South Africa was the first country with a mandatory requirement for listed companies to formulate integrated reports in response to political and environmental challenges. Integrated reporting has not been an immediate success, and effective integrated reporting will take time as organisations come to grips with changes in reporting.

These organisations, however, have to comply with recommendations to prepare an integrated report or provide reasons as to why the organisation did not prepare the report. In certain instances, organisations believe that there is no direct evidence in the worth of integrated reporting while there has been evidence that there is a positive relationship between levels of corporate social responsibility and an organisation's share price. In most cases, South African investors welcome the decision to include integrated reports for listed companies in South Africa (Atkins & Maroun 2015: 198-214). Ackers and Eccles (2015: 540) state that the King III has played a major role in the development of corporate social responsibility by South African organisations since it was released in 2009 but argue that even though there is a mandatory requirement for South African organisations listed on the Johannesburg Stock Exchange to provide these corporate social responsibility assurance practices, these King III practices have remained largely voluntary.

Marx and van Dyk (2011: 40) add that organisations need to protect and invest in the well-being of the economy because in the modern society, organisations are expected to behave in such a manner, thus making these organisations an integral part of society. There are sustainability expectations placed upon the board members of organisations as they are expected to look at sustainability needs of future generations as opposed to catering for current needs only. When organisations produce sustainability reports that are reliable and accurate, it can increase the confidence of stakeholders and the perceived legitimacy of the organisation, but there is still a gap when it comes credibility of sustainability reports produced and that one way of closing that gap is to have legislation in place governing sustainability reporting (Marx & van Dyk, 2011: 40).

The concept of information management ties in with corporate governance as there are information management regulations and legislature in place which organisations are governed by. The concept of sustainability reporting affects information management within organisations as these could result in further regulatory requirements being placed on organisations. These regulations aid in providing stability and governance which could also play a role in international investor confidence in South Africa. The topic of sustainability or corporate social responsibility comes through strongly from the authors as it is noted that the King III mandatory requirement of sustainability reporting to be done by listed companies in South Africa is still largely seen as voluntary and that organisations could falsify these reports in order unethically gain stakeholder trust and confidence. There has been said to be a need to verify and provide credibility to sustainability reports provided by organisations through implementing laws which would require organisations to have external agents verify reports. The following section looks at government law and regulations impacting the concept of information management.

### **3.3 Legislative framework on information management**

According to Malhotra and Malhotra's (2011: 45) research, consumers are concerned about the information collected on them and how it is being used and protected by organisations. More recently, governments world-wide have adopted access to information laws with the main reasons being attributed to global media growth, the technology boom, and national security issues (Relly & Sabharwal, 2008: 148). The Protection of Personal Information (POPI) Act was promulgated on 26 November 2013 by the South African government. POPI focuses on protecting the flow of information and advancing the right of access to information; if any organisation processes personal data, then it needs to be done in compliance with the POPI Act (South Africa, 2013: 34). The POPI Act can be regarded as one of the broadest privacy legislation in the world and its requirements make it difficult to fully understand the implications of the Act (Burmeister, 2014: 7).

Katos and Patel (2008: 74) argue that when government passes policy on information security and privacy, then it is of utmost importance to do this according to macro-trends as opposed to thinking on a micro-level. This allows for less contradictions that exist at the micro-level. This is explained by using the example of government's controlling the balance of spending and saving through implementing economic policies by involving macro-variables such as interest rates. Security technologies are tools, processes and methods that are used to ensure that privacy is protected (Katos & Patel, 2008: 74-76).

The Promotion of Access to Information Act (PAIA) of 2000 was assented to by the South African presidency in February 2000. This Act is “to give effect to the constitutional right of access to any information held by the State and any information that is held by another person and that is required for the exercise or protection of any rights; and to provide for matters connected therewith” (South Africa, 2000: 2). According to Wessels (2000: 12-15), everyone has access to information that is held by the state if it is required for the protection of any rights. The PAIA gives effect to the constitutional right of access to information whereby all South Africans are given the right to access records held by government institutions and private bodies.

The objectives that the PAIA looks to achieve can be summarised as follows:

- To ensure that the state takes part in promoting a human rights culture and social justice;
- To encourage openness and to establish voluntary and mandatory mechanisms or procedures which give effect to the right of access to information in a speedy, inexpensive and effortless manner as reasonably possible;
- To promote transparency, accountability and effective governance of all public and private bodies, by empowering and educating everyone to understand their rights in terms of PAIA so that they are able to exercise their rights in relation to public and private bodies, to understand the functions and operation of public bodies, and to
- Effectively scrutinise, and participate in decision making by public bodies that affects their rights.”

The Consumer Protection Act (CPA) of 2008 includes a section on the consumer’s right to privacy whereby the CPA states that every person has the right to pre-emptively block any approach or communication if the communication is for the purpose of direct marketing (South Africa, 2008: 46). According to the Department of Trade and Industry (2009: 8), consumers have the right to protect their privacy in respect to unsolicited or unwanted marketing correspondence as consumers can refuse to receive SMS’s, telephone calls, letters or spam emails and should be given the right to opt out of any of this correspondence.

In relation to records management within the justice system of South Africa, Mgoepe and Makhubela (2015: 290-291) state that the National Archives Act (NAA) no 43 of 1996 was put into law for the purpose of government areas having proper management of records and that care is taken of these public records. One of the provisions for government areas based on the NAA is to implement an electronic records system which will require a great deal of information management and information processes, procedures and systems. This is mainly paper based and struggles to deal with demands of modern society. King and Thatcher (2013: 209-212) note that in modern society, business people

are heavily dependent on technology and computers. There are, however, ethical dilemmas and to an extent, recklessness brought about by these technological computer advancements. An ethical dilemma of information technology that remains current over the years is that of software piracy or unauthorised copying or distribution of software which has become a widespread problem in the workplace. In 2010, the Business Software Alliance ordered an independent study to be conducted as it considered software piracy to be information technology's worst problem. The Business Software Alliance study in 2010 made an estimated a 35% software piracy rate in South Africa with a loss amounting 513 million US dollars. This, therefore, directly harms business producing the software as it results in loss of money and an impediment for business to produce new technologies as there may not be a financial benefit which comes from producing the new technology. This then also impacts consumers as a reduction in business profits results in higher prices being passed on to customers. As the software industry contributes to the economy, there is a negative impact on the wealth of a country as a result of piracy. In contrast, the Business Software Alliance notes that South Africa has one of the twenty lowest rates of piracy software in the world.

Mutula and Mostert (2010: 41) state that South Africa is at the top of information communications technology in Africa while being one of the largest consumers of information products and services in the world; this is because South Africa comprises the latest in fixed line, wireless and satellite communications. King and Thatcher (2013: 213-219) make mention that a big contributing factor to piracy in South Africa is as a result of an unpredictable economy. There are Intellectual Property laws in the country against software piracy, but the ease of getting away with piracy is prevalent. Software piracy is most common in countries with weak copyright and intellectual property laws. In South Africa, intellectual property is protected under the South African Copyright Act 98 of 1978. There have been nine amendments to the Act since it was promulgated. This is mainly as a result of the widespread technological advancements that have been made since the 1980s. Some organisations have their own code of ethics in relation to intellectual property and the prevention of software piracy. In a study conducted by King and Thatcher (2012) done on three organisations in Johannesburg, South Africa, software piracy was higher for people 30 years and older as well as with individuals who use computer programmes more frequently.

According to Mutula and Mostert (2010: 38-40), within the concept of service delivery, there are features of general management and financial management with a large share of service delivery describing the manner in which customer needs are met. As a result of this, South Africa and more in particularly the South African government, have in recent times seen the importance of information communications technology as well as e-government. There are regulatory frameworks being developed and policy initiatives that are being undertaken by South Africa in an effort to enhance

service delivery. In order to enhance digitally in an information driven society, there needs to be policies and regulatory frameworks. With regards to service delivery, Mutula and Kaloate (2010: 64) state that governments recognize that with the arrival of information communication technology, there is an aim to improve the levels of service delivery. Mgoepe and Makhubela (2015: 288-289) add that in relation to country's laws and citizens abiding to laws, a justice system is affected by factors which include cost, time, technological and cultural aspects as the justice system is fundamental to citizens of any country. A justice system that constantly cannot or fails to get convictions will result in citizens of the country not trusting it and having little faith in it as the conviction rate is a way of measuring the success of a justice system.

Based on the increase in consumer awareness on how their information is used and protected by organisations as well as other factors such as technology advancements as stated by the authors, governments have specific laws and regulations for organisations to abide by pertaining to customer information. POPI is the most recent information-related Act signed by the South African presidency; however, organisational heads may still need to come to terms with what it means for their organisations. The CPA focuses more on the rights of a consumer when purchasing goods and services but makes mention of direct marketing. Therefore, the concept of information management which relates to this study (while the PAIA which has been in existence for longer) is aimed at citizens' rights to access information. Organisations also need to comply with the PAIA even though it less focused on organisations compared to POPI.

These Acts on privacy and protection for consumers are relevant to the study of information in corporate organisations and the information management systems and policies of these organisations as it would need to be aligned and compliant to these government Acts. Laws of intellectual property and piracy have also come through strongly with a big focus on how a country's justice system can impact on individuals and organisations abiding by these laws. It is said that in South Africa, the ease of getting away with piracy is rampant, which increases the likelihood of individuals to not act in accordance to the law when it comes to piracy. The concept of piracy ties in with information management as organisations require their policies and procedures to include piracy and the use of software.

Piracy could also impact the organisation's profits, thus impacting the economy. It is noted that the South African government does recognise the use of information technology to improve service delivery and that in order to enhance service in a data-driven society, the government needs to put in place a legal framework around information and how this used and managed in a digital format. This study reviews government legislation and organisational policies at a financial institution in South

Africa and analyses if employees are aligned and aware of these government legislation and organisational policies as organisational information is used on a daily basis by employees. Information structure and the use of information in South African organisations is discussed in the next section.

### **3.4 Information structure and use in South African organisations**

Straus and du Toit (2008) state that South Africa has a lack of global competitiveness which has in more recent times become a topical issue. Competitive intelligence is a tool to readdress these inadequacies by taking information and converting it to insights that could be used by management to make strategic decisions for the organisation. There has been an increase in organisations looking at the need to use and interpret both internal and external information in order to understand the full picture and make strategic decisions. As a result of technological advancements, organisations can now have more information available to them much quicker and easier than before and therefore, organisations require competitive intelligence to make sense of this information. South Africa and other African countries still do not proactively make good decisions as a result of changes in the environment as managing information intelligence is still mainly unknown to organisations in these areas; therefore, competitive intelligence sits low in the structure of South African organisations (Strauss & du Toit, 2008: 302-307).

Heppes and du Toit (2009: 48-54) add that in order to sustain a competitive advantage, management requires competitive intelligence as strategic management must evaluate the external environment in an accurate manner. Organisations need to evaluate information in relation to the activities of its competitors as well as business trends in order to achieve its own organisational goals; there are five key components of competitive intelligence, namely: obtaining competitive intelligence requests, collecting information, analysing and synthesising information, communicating intelligence and managing the competitive intelligence process. In South Africa, competitive intelligence is done on a small scale while organisations do recognise the need to integrate competitive intelligence into its business and strategy as South African retail banks and financial services operates in a complex and vigorous environment that has gone through major changes following the introduction of the democratic government in the 1990s.

This has come with new regulatory requirements while foreign financial services companies have also entered the South African market. An empirical study done by Heppes and du Toit (2009: 54-64) on a South African retail bank with the purpose of assessing the level of maturity of competitive intelligence found that the competitive intelligence maturity was at mid-level, with there being significant opportunity for it to develop to global high levels.

Mutula and Mostert (2010: 43-44) note that there are a number of challenges that South Africa faces to effectively roll out e-government programs in spite of the information communications technology infrastructure, policy and legislative frameworks. A survey conducted by the United Nations in 2008 on e-government ranked South Africa 61 out of 192 members. There are also some challenges faced on information communications technology mainly said to be the lack of support for strategic policy decision-making and programmes designed to influence information communications technology for information development in South Africa. According to Strauss and du Toit (2008: 303), major barriers to economic growth in South Africa include high telecommunications costs and skills shortages, and issues of skilled shortages and poor services have not been addressed by the government, which leads back to inadequate government policy. Katuu (2012: 39-52) notes, in a research on enterprise content information to provide a picture of the enterprise content information in South Africa, that among both the private and public sectors, there are several requirements needed to address the skills shortage in the South Africa in relation to enterprise content information in organisations.

Enterprise content information encompasses: document management, records management, process management, collaboration, imaging, knowledge management, digital asset management, digital rights management, web content management and portals. There are further debates as to how many components enterprise content information actually has. Enterprise content information is, therefore, inclusive of strategies, tools and methods in order to manage content while on the African content, South Africa is the most advanced country on enterprise content information implementations.

According to Mutula and Kaloate (2010: 64-78), the use of open source software helps to achieve delivery as it comes with a lower cost than commercial based software. Open source software that is free from propriety restrictions which can be modified by people to suit their organisational needs without having to pay software companies any additional charges; with open source software, people are able to view the underlying code and modify it to the requirements of the organisation. When comparing South Africa to developed as well as other developing countries, it was found that there is a limited use of open source software in the public sector. (Chikandiwa, Contogiannis and Jembere, 2013: 365-377) make reference to social media use by organisations as a form of communicating information to customers as well as a form of target marketing as it presents an opportunity for organisations to engage and interact with customers and extract information to be used for marketing intelligence, which banks can strategically make use of.

There is a need in today's environment to use social media as a platform for customer relationship management as well as integrate strategic marketing strategies and communication. In South Africa,



there has not been much adoption of social media by banks, and there follows a similar trend in the rest of Africa. The model proposed to implement social media in organisations is categorised under models that prioritise the target audience, models that prioritise the organisations strategic objectives and models that try to strike a balance between prioritising audiences and strategic objectives. As a result of the regulatory and legal policies put in place to protect customers, the banking sector has been seen to be particular about information sent to customers. This could therefore pose a challenge to banking and other financial organisations who wish to adopt social media as part of their broader information strategy. Most South African banks who have some sort of social media strategy have this social media strategy managed and administered by a single department and have thus not decentralised this to other departments while some managers believe that social media should be managed by a special group of people.

The authors make reference to the need for South African organisations to make use of competitive intelligence in their companies as this is required to gain a competitive advantage. With so much information available to organisations combined with the fast pace at which information is received as a result of improvements in technology, it is said that it is imperative for strategic management to make use of this information in an effective manner. Competitive intelligence is still largely unknown within South African organisations or is done on a small scale and sits low in their structure. Therefore, these organisations find it hard to integrate competitive intelligence into the mainstream of their business. In multiple cases, it has been noted that there are large areas of improvement for organisations to make, in particular, banks - to use information and competitive intelligence to better their business. In order to use information communications technology to better organisations in South Africa, it has been found that a lack of skills and the high cost of telecommunications have hampered this and that inadequate government policies play a large role in these barriers.

There has also been a lack of enterprise content information in South Africa, thus affecting document management, records management, process management, collaboration, imaging, knowledge management, digital asset management, digital rights management, web content management and portals as this is what enterprise content information covers according to certain authors. In the same light, the use of information by organisations on social media is done on a low scale in South Africa, which can be partially attributed to the dynamic laws and policies in the country when it comes to consumers' rights. Social media is said to be a powerful tool that could be used to market to customers thus using and relying on information to segment target audiences. This study reviews how information is viewed by respondents at a financial organisation by assessing the importance of information and how information is treated at the organisation.

Furthermore, all the areas covered under this section namely: competitive intelligence, enterprise content management, skills shortages, software and social media relate to this study as they all require information management structures and data structures. Competitive intelligence involves taking information and converting it to insights for strategic decision making, in combination with technological advancements, thus making it easier for organisations to use this information. Therefore, the organisation requires strategies on the management of information, specifically in the private sector, as organisations need to be competitive in order to survive. These strategies on information management formulated by organisations are important as this information is used to achieve organisational goals. The fact of skill shortages in enterprise content management and generally, skill shortages in South Africa is noted by authors. This affects the information structure and the use of information in South African organisations which, in turn, affects how South African organisations use information for daily operations and how information is used for strategising in organisations.

Enterprise content management speaks to organisations managing content through processes and tools and ultimately, a technology system or systems. In this study, the use and capability of systems is reviewed in relation to information management while enterprise content management could benefit the organisation; therefore, technology systems and organisational processes would be affected if enterprise content management is adopted. It is noted by the authors that software and social media could be used for market intelligence. This concept ties in with this study since as a pre-requisite for organisations to use software and social media, information structures would need to be in place at the organisation because using software or social media will mainly be the execution platform to speak to customers. The underlying data and information structures, as well as this data and information being available and easily accessible in the company will be what drives the marketing intelligence. The next section investigates information management policies and procedures of a selected South African financial institution in order to provide context on what internal policies and procedures exist at the organisation.

### **3.5 Information management policies at a selected South African financial institution**

At a selected financial institution, there is an information system acceptable use policy guide that must be signed by all employees and vendors who are given access to any of the company systems. This policy is also made available to employees on the organisation's intranet. This policy guide aims to (nd: 2015):

- To promote the professional, ethical, lawful and productive use of the organisations information systems;

- To define and prohibit unacceptable use of the organisations information systems;
- To educate users about their Information Security responsibilities;
- To describe where, when and why monitoring may take place; and
- To outline disciplinary procedures.

This policy reviews the principles of information security as (nd: 2015):

- Information is an asset, like any other business asset it has a value and must be protected;
- The systems that enable us to store, process and communicate this information must also be protected;
- 'Information Systems' is the collective term for our information and the systems we use to store, process and communicate it; and
- The practice of protecting our information systems is known as 'Information Security'.

The main principles that the policy highlights to employees and vendors are summarised as follows (nd: 2015):

- All employees share the Information Technology facilities at the organisation and it is the employee's responsibility to contribute towards keeping this information safe;
- These facilities are provided to employees for the purpose of conducting company business;
- These facilities must be used responsibly by everyone, since misuse by even a few individuals, has the potential to negatively impact productivity, disrupt company business and interfere with the work or rights of others;
- Therefore, all employees are expected to exercise responsible and ethical behaviour when using the company's Information Technology facilities;
- Any action that may expose the organisation to risks of unauthorized access to data, disclosure of information, legal liability, or potential system failure is prohibited and may result in disciplinary action up to and including termination of employment and/or criminal prosecution;
- The organisation reserves the right to monitor, intercept and examine email messages, files on personal computers, internet traffic and any other information stored on or passing through organisations computers;
- Exercise care and comply with all guidelines as stipulated in this information security policy;
- Protect the organisations data integrity and computing facilities against unauthorized access or improper use; and
- Report users whom you think do not comply with the guidelines as stated in this policy.

Another document available on the organisation's intranet is the organisation's IT security policy. The purpose of the IT Security policy is to prescribe mechanisms that help identify and prevent the misuse of organisational data, applications, networks and computer systems, and to define mechanisms that protects the reputation of the organisation and allows the organisation to satisfy its statutory and ethical responsibilities. The areas that the policy covers are can be summarised as headings:

#### 1. Security management;

- The business owns information and is therefore accountable for its confidentiality, integrity and availability;
- Business, users, IT staff and third parties are custodians of information and is responsible for protecting information in terms of business risk;
- The business decides who may have custody of information;
- The business classifies information in accordance with the potential harm that the business may suffer in the event of security incidents;
- The business is responsible for ensuring that information custodians protect data in accordance with its classification;
- Disclosure of classified information to the press or news media requires approval from the business owners of the information; and
- All employees, contractors and third parties will attend appropriate awareness training and familiarise themselves regularly with updates in policies as relevant for their job function. The organisation will have, in place, processes and procedures, which will enable all employees, contractors and third parties who are not able to understand this policy to enquire with management and have the policy explained to them in a language and in a manner that they understand. In the event that the employees, contractors and third parties are not able to understand this policy they are required to report their lack of understanding to management.

#### 2. Information handling

All organisational information must be classified by the business according to its sensitivity to ensure that appropriate controls are applied during its creation, storage, processing and disposal. The classification criteria is to be used for all information, whether electronically stored, paper- based, or intellectually retained (nd: 2015).

#### 3. User access for employees, contractors and third parties

Access to the organisation's information systems must be restricted to those entities that have a legitimate business need and have been specifically authorised or granted through an approved process. Individual accountability must be assured at all times (nd: 2015).

#### 4. Business applications

Systems development and maintenance must be carried out in a way that ensures robust secure systems and meet business requirements (nd: 2015).

#### 5. Infrastructure and networks

- Network devices may not be connected to the network until baseline controls have been implemented on the technology;
- Any device connected to an external or untrusted network and the internal or trusted network simultaneously must be seen as a network perimeter. This device must therefore be protected in line with baseline controls;
- The network perimeter must be controlled to manage the risk of access from external threats;
- All connection points with the Internet, non-group companies, or with other group companies not managed by the organisations network team, must be protected by firewall technology. Firewalls must be configured to restrict inbound and outbound traffic to that which is necessary and secure, in terms of current good security practice;
- Wireless access to the organisations network must be secure and comply with baseline controls;
- Information must be backed up in a secure and reliable manner to ensure that business operation is not impaired in the event of information loss.
- Formal backup failure response procedures are required;
- All systems connected to the Internet must be current with security patches and must have additional vulnerabilities identified and resolved; and
- Devices on the network (e.g. desktops, laptops, servers etc.) must comply with the group naming conventions so that Group network custodians can identify the business area responsible for any device on the network which may pose a risk (nd: 2015).

#### 6. Security Incidents

- All transactional systems, or systems that process any information rated “Confidential” or higher, must retain event logging that enables the ability to identify user access and the reconstruction of transactions performed. This can be done through any combination of front-end and back-end logging provided it is always possible to link events needed. It is recommended that an external logging monitoring functionality should enable detection of sensitive database “dumps” ; and

- All users will be made aware of their responsibility to report security incidents or suspected vulnerabilities on a timely basis (nd: 2015).

## 7. Legislative compliance

Information systems environments may be subject to legal and regulatory requirements (including cross-border requirements) in any country where they are used (nd: 2015).

The policies of this financial institution cover various aspects of information management and information systems. The information system's acceptable use guide policy aims to give employees and vendors an overall high level breakdown of what is acceptable and not acceptable in terms of information systems and information as this classifies information as an asset of the organisation. This policy makes it clear that there is an onus on the employee to protect and not misuse company information while making mention to possible disciplinary action that could take place should an employee contravene the policy. The IT security policy provides substantial and more in-depth detail to what is required from employees and the business in terms of various information management related areas such as security management and business applications used by the organisation. This breakdown identifies internal policies in relation to information management at this organisation.

## 3.6 Summary

In reviewing laws in South Africa; there have been a number of new laws and amendments to laws and legislations in the country. These have been driven mainly by the new democracy which was established in the 1990s and the rapid advancement of technology which is continuing to have an impact on the way organisations do business. These technological advancements and more particularly; the information that is now available to strategic managers play a major role in the decisions that these managers make for their organisations in order to be competitive. It has however, been noted by various authors and researchers that South Africa is not up to speed when it comes to the overall management and business strategy to get this valuable information to the hands of strategic managers. The trend seems to be the same across Africa, with it said that South Africa is the most advanced on the African continent when it comes to this concept of competitive intelligence. Law enforcers in South Africa have come up short, from the perspective of the authors, as it comes across that the ease of not being convicted as well as laws not being strict enough have heightened individuals not abiding by laws such as piracy laws. Globally, in both developed and developing countries, there have been laws put in place on information. Developed countries do, however, seem to be steps ahead when it comes to using information as part of the strategic decision-making tools for the organisation. The concept of privacy and consumer protection is gaining momentum as there are various government legislations such as the Consumer Protection Act and more recently, the

Protection of Personal Information Act which requires organisations to comply with state laws in terms of how customer information is processed and used. These government laws need to be incorporated into an organisation's policy and procedures guide in order to ensure that the organisation and its employees align themselves to these laws. When looking at the information management policies of a selected South African financial institution, the policies provide an in-depth guide to what is expected from employees and the organisation in terms of IT security and protecting organisational information, but it can be argued that the policies do not take into account all aspects of POPI or CPA laws. Whether these laws are being adhered to or taken into account by the organisation cannot be determined by these policy guidelines that the organisation has available. Whether individual departments are adopting certain aspects of the laws relating to their business unit cannot be identified by these policies. This study reviewed and analysed which government policies and legislation the organisation is aligned to as well as determined strategies adopted by management of the organisation in relation to information management and information management policy and procedure. The chapter that follows explains the research methodology used for the empirical investigation as well as highlights ethical considerations taken into account when conducting a research study.

## **CHAPTER FOUR: RESEARCH DESIGN AND METHODOLOGY**

### **4.1 Introduction**

This chapter explains the research methodology and design that guide the objectives and interrogations of the research. This research is exploratory in nature. This empirical study investigated information management systems at a selected financial institution. The research questions and objectives are presented in the chapter as well as how the sample population for the research study was selected. Both qualitative and quantitative research methods were used to carry out the required research. The data collection techniques used for this study were questionnaires and semi-structured interviews. This chapter further constitutes discussion on research reliability and validity testing that the research took into account, including some of the ethical considerations that the research is governed by.

### **4.2 Focus of the study**

The study was triggered by the increase in information breaches in organisations. Organisations may have policies and procedures, strategies and systems in place to mitigate the risk of information breaches, but data breaches are still on the rise. Governments across the world have or are putting in place laws around data protection which organisations have to align their process, strategies and systems to.

There is a perception that financial institutions are weak based on the number and severity of information breaching incidents and financial institutions failing to secure personal information. Sujatha (2011: 137-138) argues that one of the main problems addressed by consumers in the banking industry is their concern about identity theft and hackers, fraudulent activity and security threats. A phishing attack was launched on a leading bank in India whereby customers were asked for personal details (Gupta, 2012: 243). Based on the authors' research, information breaches and the security of information is a big concern for consumers, and organisations in the financial industry are not completely secure when it comes to protecting customer information through their systems.

### **4.3 Research objectives**

The primary objectives of this study are as follows:

- To explore the shortfalls of information security on a South African financial institution.
- To investigate if data remains separate and privacy is ensured.
- To investigate responsiveness of business processes on information management.
- To investigate the capability of systems on information management.
- To investigate the strategies formulated for information management.



- To investigate projects and programmes aimed at addressing information management.
- To investigate contingency plans on how to respond to the financial risk in respect to information management.
- To provide recommendations based on the empirical findings.

#### **4.4 Research questions**

The study was guided by the following questions:

- What are the shortfalls of information security in a selected South African financial institution?
- Are institutional contingency plans (preparedness, mitigation, response and recovery) effective for any forthcoming risk?
- What changes does the organisation need to consider adopting as a result of information security?
- How are the various value chains of the organisation affected by information security?

#### **4.5 Research approach**

In order to have a well-structured research model, the research has to be complete or well rounded to the context and be conceptually innovative and methodological while also committing to building theory in a cumulative way (Luker, 2008: 3). Furthermore, methodology is a design used in research for data collection and analysing procedures to investigate a research problem (McMillan & Schumacher, 2008). The integration of qualitative and quantitative research has become a formalised approach in conducting research as this mixed method approach to research has certain advantages (Bryman, 2006: 98). This integrated approach involves strategies of collecting data either simultaneously or sequentially in order to best understand the research problems (Creswell, 2003: 18). This approach of using both a qualitative and quantitative approach was adopted in this study in order to best understand the research problems.

A structured questionnaire was distributed to the research participants at different employment levels. These levels are aligned to the level of the organisation in study. The employment levels for the questionnaire consist of middle management, non-managerial specialists, lower level management and agent level staff. A questionnaire is an important tool as it collects responses and data for analysis to achieve the purpose and objectives outlined. In-depth interviews were conducted with management at strategic levels of the institution. In-depth interviews allow for rich data to be extracted for analysis. These strategic level managers are classified into two levels namely: executive management and non-executive senior management. Functions of these executive management and non-executive

senior management include ensuring that the appropriate policies exist for the organisation and also form company goals and strategies. This research is guided by the research questions and research objectives. Furthermore, Collis and Hussey (2009: 4) state that research studies are also guided by the purpose of the research, process of the research, logic of the research and outcome of the research.

#### **4.6 Sampling procedure and description of the sample**

A sampling procedure is followed to collect information from a population and refers to a process used to select a portion of the population for study purposes (Nieuwenhuis, 2007: 73). Neelankavil (2007: 234) explains that it explicitly explains the sampling process to consist of defining the population, obtaining a list of the population, selecting a sample frame, determining the sample methods, developing a procedure for selecting the sample units, determining the population size and drawing the sample. There are various types of sampling techniques used in research while some of these include stratified sampling and purposive sampling.

According to Teddlie and Yu (2007: 79), stratified sampling involves getting a representative sample of the population on some characteristic of interest while in random sampling, the accessible population has an equal chance of being selected. Holloway and Wheeler (1996: 74) describe purposive sampling as sampling where individuals or groups with special knowledge of a topic are chosen for the research study. According to the Australian bureau of statistics (2013), whether taking a census or selecting a sample, both of these methods give the researcher the ability to draw conclusions about the whole population. It is further explained that a census studies every unit or everyone in a population and is known as a complete enumeration while a sample is a subset of units in a population selected in order to represent all units in the interested population of the researcher and is known as partial enumeration. For the quantitative research portion of this study, a census was conducted. This is important as all individuals who are not part of the strategic management group were deemed selectable to partake in the study. The researcher attempted to get responses from all of these individuals. Non-probability sampling was used for the in-depth interviews as certain individuals who hold senior management positions were identified. This is important as these individuals are involved in creating policies and aligning government regulation with organisational policies. Non-probability sampling is further explained in section 4.6.3.

##### **4.6.1 Population**

Current staff members of a selected financial institution in South Africa were included for this research study. The population consisted of staff members across the value chain and comprised staff members holding various positions in the organisation. The positions are categorised based on the

organisational structure of the organisation. As highlighted previously, these positions or levels are: executive management, non-executive senior management, middle management, non-managerial specialists, lower level management and agent level staff.

#### **4.6.2 Sampling for the quantitative research method**

A structured questionnaire was distributed to employees in all value chain areas of the organisation. Oppenheim (2000: 10) states that a questionnaire is not just a list of questions or form to be filled in but that it is essentially a measurement tool and more specifically, an instrument for data collection. For this study, the questionnaire was distributed by sending the questionnaires via email to all middle managers in the organisation for them to distribute to their staff members and also printing out questionnaires as a follow up to the email and giving these to these managers for them to distribute to their staff. There were multiple middle managers within the same value chain of the organisation, and all of these middle managers were given the questionnaire to distribute to staff.

Specialists and middle managers were emailed directly by the researcher asking them to partake in the research by completing the questionnaire with follow up request emails sent to those who did not respond. Senior, strategic managers were not asked to partake in the questionnaire as interviews were conducted with these managers, discussed further in section 4.6.3. As explained previously, a census approach was used. As not all managers would pass on the questionnaires to their staff and for those managers who did distribute the questionnaire to staff, some staff would ignore the questionnaire as it is not mandatory to respond or partake in the research; therefore, it is estimated that approximately 500 employees received the questionnaire. All individuals at the organisation were affected by information policies. The sample size used in the research represented all areas of the value chain in the organisation. Most individuals of the organisation deal with organisational information being it customer information or the organisation's financial information. There were 81 questionnaires that were returned as part of the quantitative data collection (Refer to Appendix A for raw data analysis results). Attention was applied to the reliability and validity of all research, without this, the research can become fictional and lose its utility (Morse, Barret, Mayan, Olson & Spiers, 2002:14).

#### **4.6.3 Sampling for the qualitative research method**

Holloway and Wheeler (1996) described purposive sampling as noted previously. Trochim (2006) describes this in more detail by stating that non-probability sampling methods are mainly of a purposive nature as there is a specific plan in mind to sample the problem. The above-mentioned author further explains non-probability sampling as sampling that does not involve a random selection

to identify the population. In this research, non-probability sampling was used to select strategic management members across the organisation. In-depth interviews were conducted with these managers who occupy strategic positions. Strategic management sets organisational policies relating to information management. Different strategic managers were selected as each manager could look at a different aspect of information management such as information technology systems or policies on information within the organisation. Managers interviewed include: the senior manager of compliance and operational risk, head of information technology, head of data, senior manager of collections, head of human resources, senior manager for information technology operations, senior manager for decision technology, senior manager for information architecture and senior manager of value added products. These individuals were selected as strategic management develops strategies which filter down to middle and lower level management and eventually, staff level employees. It is also important to get senior management involved in discussions.

According to Zwikael (2008: 387), it is of high importance to get the support of top management when conducting projects. Furthermore, Ko and Fink 2010:662) and Hagmann (2013: 229) state that senior management provides the necessary direction for the organisation and that in order to have synergies of information in the organisation, executive and senior management need to support strategies of information and information governance whereby all business areas need to be involved. Nine (9) strategic management members from different areas of the organisation were interviewed (Refer to Appendix B for printout of questionnaires).

#### **4.7 Data collection**

Interviews refer to a data collecting method whereby qualitative or quantitative questions can be asked; the qualitative questions are open-ended whereby participants respond in their own words (Doody & Noonan, 2013: 28). Structured questionnaires were self-administered by the researcher to the research participants. In-depth interviews were conducted with senior management of the organisation in order to gain richer information while still following a structured set of questions to be asked. A structured questionnaire was used to gather information from staff level members of the organisation and measured through the Likert scale. The items were measured using a five-point Likert scale which was developed with a range from (1) strongly disagree, (2) disagree and (3) undecided to (4) agree and (5) strongly agree, thus testing the perceptions of the leaders through leading statements. Using this approach should enrich the findings and lead to a strong view on the current state of information management within the organisation and the challenges that need to be overcome to transition into a higher level of organisational compliance. A questionnaire is an important tool for data collection as Pawar (2004: 28) states that questionnaires allow researchers to reach out to respondents whilst maintaining confidentiality and anonymity. The Likert scale is effective as Chin,

Johnson and Schwarz (2008) mention that when a Likert scale is used, it allows respondents to offer subjective responses of their opinions and attitudes.

The biographical information used in the data collection instruments included: gender, age, level of education, staffing level and length of service in the respondent's current position. The dimensions used included: breaching of data in a financial institution, information management mitigation in a financial institution, information management preparedness in a financial institution, information management systems in a financial institution and information management risk response and recovery in a financial institution. The instruments were mainly informed by the literature reviewed on information management and data breaches in conjunction with the objectives of the research study. The questionnaire was distributed via email or hand delivered to managers and returned to the researcher via email or as a hard copy and then scanned and emailed to the researcher's computer. According to Ruane (2004:131), closed-ended or restricted questions provide a limited number of response alternatives for respondents to select from while Cohen, Manion and Morrison (2007: 338) add that a questionnaire is designed in a simple and clear manner, thus allowing respondents to easily complete the questions listed. Furthermore, Burns and Grove (2009: 43) describe data collection as a precise and systematic gathering of information relevant to the purpose of the research. The questionnaire consisted of 64 items with a level of measurement at a nominal or an ordinal level. The questionnaire was divided into 6 sections which measured various themes as illustrated below:

Section A – Biographical information

Section B – Breaching of data in a financial institution

Section C – Information management mitigation in a financial institution

Section D – Information management preparedness in a financial institution

Section E – Information management systems in a financial institution

Section F – Risk response and recovery in a financial institution

#### **4.8 Piloting**

Pilot studies are usually put forward as a test in order to test and refine aspects of the study (Yin, 2011: 37). In this research, a pilot test was performed on the questionnaire whereby three participants from different areas of the organisation completed the questionnaire in order to determine how long the questionnaire took to complete and whether the questions posed any difficulty in completing. The three respondents completed the questionnaire within a time of 15 to 20 minutes and understood the flow of the questionnaire. According to Sampson (2004: 83), this preliminary fieldwork is important as it helps to identify issues such as ethics and research validation.

A pilot test was performed on the interview questions whereby one senior management participant was interviewed in order to determine whether the questions posed any difficulty in terms of understanding. The length of the interview was not a factor as different participants would provide longer or shorter answers to the interview questions. The result of the pilot was that the interview questions did not need refinement as the interviewees understood the questions asked by the researcher. The latter participants to the interviews, after the pilot study, were all senior management members. According to Holloway (1997: 121), when doing a pilot study in qualitative research, pilots are not of utmost importance as there is flexibility for the researcher to learn on the job while Silverman (2010) argues that mainly with interviews in qualitative research, pilots help with certain aspects of the research design whereas Sampson (2004: 400) adds that pilots is a test to an unknown environment.

#### 4.9 Quantitative data analysis

The raw data collected from the questionnaire was statistically and descriptively analysed. IBM data analytics software was used to provide descriptive data for analysis. SPSS version 23.0 was used for quantitative analytics. According to Zaman (n.d), SPSS is a leading software for providing predictive analytics with a long history of statistical analysis. The Likert scale uses a five-point scale to measure responses (Clason & Dormody, 1994). The Likert scale categorises responses under five classifications namely: strongly disagree, disagree, undecided, agree, and strongly agree. The results there of provided by the statistician was analysed and presented by the researcher using descriptive statistics to quantify the data in line with the research study’s main objective. Factor analysis was used with the main goal of data reduction. According to O’Rourke and Hatcher (2013:47), factor analysis can be used when the researcher has obtained responses to several of measures and wishes to identify the number and nature of the underlying factors that are responsible for co-variation in the data.

**Table 4.1: Biographical Frequencies**

<b>Gender</b>		
	Frequency	Percent
Male	31	38
Female	50	62
Total	81	100
<b>Age</b>		
	Frequency	Percent
21 - 30	41	51
31 - 40	32	40
41 - 50	8	10
Total	81	100
<b>Highest level of education completed</b>		
	Frequency	Percent
Matric	24	30

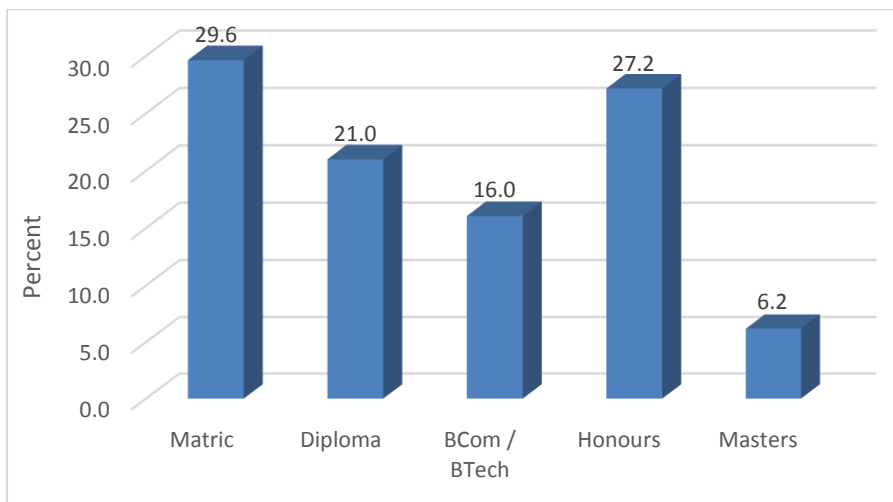
Diploma	17	21
BCom / BTech	13	16
Honours	22	27
Masters	5	6
Total	81	100
<b>Staffing level</b>		
	Frequency	Percent
Middle Management	21	26
Non Managerial Specialist	32	40
Lower Level Management	10	12
Agent Level	18	22
Total	81	100
<b>Area of Specialisation</b>		
	Frequency	Percent
Collections	4	5
Compliance/Legal	4	5
Credit Risk	17	21
Finance	6	7
Information Technology	14	17
Human Resources	5	6
Marketing	9	11
Operations	22	27
Total	81	100
<b>Length of Service</b>		
0 -3 years	63	78
4 - 6 years	15	19
7 - 10 years	2	2
> 10 years	1	1
Total	81	100

Table 4.1 displays the frequencies generated from the biographical information of the questionnaires. The biographical data of the frequencies are discussed in more detail below.

**Table 4.2: Gender to age ratio**

		Gender		Total	
		Male	Female		
Age (years)	21 - 30	Count	15	26	41
		% within Age	36.6%	63.4%	100.0%
		% within Gender	48.4%	52.0%	50.6%
		% of Total	18.5%	32.1%	50.6%
	31 - 40	Count	14	18	32
		% within Age	43.8%	56.3%	100.0%
		% within Gender	45.2%	36.0%	39.5%
		% of Total	17.3%	22.2%	39.5%
	41 - 50	Count	2	6	8
		% within Age	25.0%	75.0%	100.0%
		% within Gender	6.5%	12.0%	9.9%
		% of Total	2.5%	7.4%	9.9%
Total	Count	31	50	81	
	% within Age	38.3%	61.7%	100.0%	
	% within Gender	100.0%	100.0%	100.0%	
	% of Total	38.3%	61.7%	100.0%	

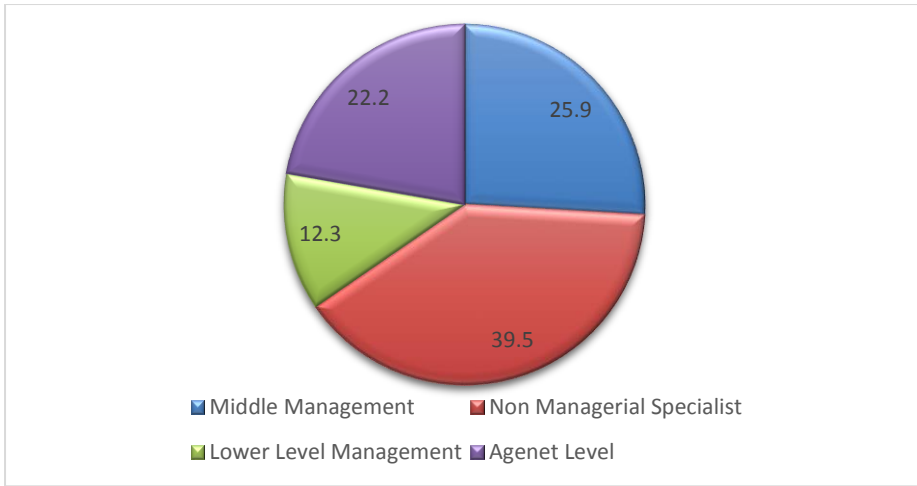
There were more females than males that partook in the quantitative portion of the study with a percentage of 38% for males to 62% for females. The number of females in the professional workplace seems to be on the increase. This is echoed in the literature by Hausmann, Tyson and Zahidi (2009: 27-30) whereby they state that the gender gap has closed whereby males previously outnumbered females. Within the age category of 31 to 40 years, 43.8% were male. Within the category of males (only), 45.2% were between the ages of 31 to 40 years. This category of males between the ages of 31 to 40 years formed 17.3% of the total sample. Authors such as Hertel, Van der Heijden, de Lange and Deller (2009: 858) and Niessen, Swarowsky and Leiz (2010: 356) have noted that workers over 50 are remaining as part of the workforce for longer periods than before. It is, however, stated that the average age of employees at the institution in study is 28 years of age (n.d. 2015). This correlates to the ages of the respondents in this study.



**Figure 4.1: Classification of education levels**

Figure 4.1 above displays the education levels of the respondents from the questionnaires. More than 70% of respondents had a post-school qualification. A third of the respondents had a post-graduate degree. This is a useful statistic as it indicates that a fair proportion of the respondents have a higher qualification. This indicates that the responses gathered would have been from an informed (learned) source. Verhofstadt, De Witte and Omeij (2007: 135) noted that jobs with less physical demanding job characteristics are, more often, filled by workers who are educated at a higher level. This speaks to the distribution of education levels at the institution as working in a financial institution constitutes a job that is less physically demanding in comparison to a brick layer where work tasks are more physically demanding.





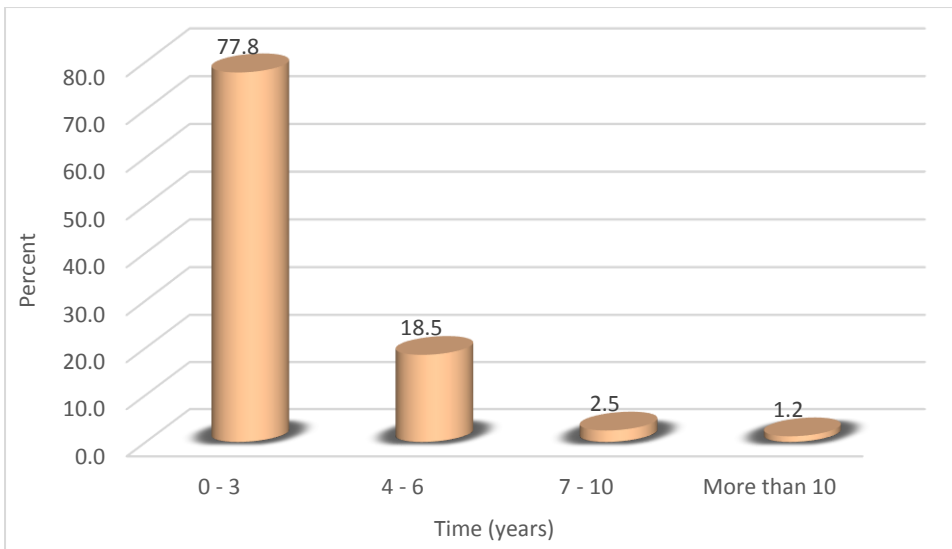
**Figure 4.2: Classification of staffing levels**

The nature of the positions held by the respondents is shown in Figure 4.2. This is from the questionnaires whereby 38% of responders were management in the organisation. This comprises lower and middle level managers since senior managers formed part of the semi-structured interviews and not the questionnaires. There is a large number of specialists who responded to the questionnaire while almost ¼ of respondents were agent level employees. According to Peters and Zelewski (2007: 84-85), employees should be assigned jobs based on their competencies as this will result in an efficient job performance. However, it is also noted that employees could have been assigned to a job based on the employees’ preference regarding the competences.

**Table 4.3: Areas of specialisation**

	Frequency	Percent
Collections	4	5
Compliance/Legal	4	5
Credit Risk	17	21
Finance	6	7
Information Technology	14	17
Human Resources	5	6
Marketing	9	11
Operations	22	27
Total	81	100

The areas of specialisation from the questionnaires are shown above in Table 4.3. The majority of the respondents (27%) are from the operations area. This is in line with proportion of employees in the divisions as operations hold the most number of employees at the organisation. All areas of the organisation were involved in this study as highlighted previously by Gal and Berente (2008: 133) that implementing information systems is a complex process whereby all stakeholder groups have to be involved as their understanding or perception of the technology may be different.



**Figure 4.3: Classification of length of service**

Figure 4.3 above indicates the length of service of the respondents from the questionnaires. Three-quarters of the respondents (77.8%) had been in employ for less than 3 years. As many of the respondents are in managerial positions, this implies that respondents had been in employ for a while, and this is also a useful fact as it indicates responses from experienced workers. It has been mentioned previously by D'Arcy and Green (2014: 484) that the amount of time that an employee has been employed at the organisation also plays a role in employee security compliance while Abu-Musa (2012:226-227) added that information security should involve the necessary management and should just not be seen as a technical issue. Analysis from the rest of the frequencies is covered in chapter 5.

#### **4.10 Qualitative data analysis**

The data collected from the research study's semi structured in-depth interviews was analysed whereby patterns were identified and trends categorised into themes in line with the research study's main objective. The managers interviewed included: the senior manager of compliance and operational risk, head of information technology, head of data, senior manager of collections, head of human resources, senior manager for information technology operations, senior manager for decision technology, senior manager for information architecture and senior manager of value added products. There were more males than females who took part in the interviews, of the 9 interview respondents, 7 were male while 2 were female. Moreover, 3 respondents were between the ages of 31 to 40 while 2 respondents between the ages of 41 to 50; 3 respondents were between the ages of 51 to 60, and 8 of the 9 respondents had a tertiary level education. The table above further shows that 1 respondent's highest level of education was matric (grade 12), 1 respondent had a B-com degree, 4 respondents had an honours degree, while 3 respondents had a Master's degree. Of the 9 senior

managers, 3 respondents were executive level senior management and 6 were non-executive senior level management. The majority of the respondents (7) had been employed in their position at the organisation for 0 to 3 years, 1 respondent was employed between 4 and 6 years and another 1 respondent had been in employ for 7 to 10 years. Analysis from the rest of the dimensions is covered in chapter 6.

#### **4.11 Research reliability and validity**

In this research, there was testing conducted on the reliability and validity of the data and findings in order to check its applicability, consistency and neutrality. Morse et al. (2002: 13-14) note that there has been an increase in requiring 'rigour' during the course of research whereby strategies for evaluating trustworthiness need to be implemented in order for the research not to lose its utility "hence, a great deal of attention being applied to reliability and validity in all research methods". Collins and Hussey (1997: 55) state that the reliability of open-ended questions is low in comparison to the higher validity of using closed-ended questions as generalisations can be construed and used in different settings with a lower reliability. The research questionnaire used for this study consisted of close-ended questions which provided reliable data as respondents were required to select responses from pre-defined listings. The interviews were recorded by the researcher with the consent of the participants. All interview participants were asked the same questions. Cooper and Schindler (2003: 231) state that the demographic and enterprise data completed by the respondents are reviewed against the research delineation to ensure the respondents are aligned to the research delineation while Fraenkel and Wallen (2001) add that an instrument is valid if it measures what it is intended to measure and accurately achieves the purpose for which it was designed.

#### **4.12 Ethical considerations**

Whilst conducting research, there are certain ethical behaviour and considerations that the researcher should take into account (Polonski & Waller, 2010: 53). Polonski and Waller (2010) explain that the participants who assist in providing information should do so voluntarily and must be informed if there are any anticipated negative consequences as a result of the participation. There should be no force or deception in getting potential participants to partake in the research. Confidentiality should be practised whereby the identity of the participants is not revealed in the consequential report. If a researcher works in a particular industry, then the researcher should avoid looking at competitors as this could cause a conflict of interest. If this is done, the researcher must make mention of the dual status as a researcher and a competitor. Saunders, Lewis and Thornhill, (2000: 138) state that if consent is not granted by the respondent, then the respondent should not be forced to give a response while Fox and Ritchie (n.d) add that when engaging with participants, the rationale of the research

must be clearly communicated as well as determine whether the participants require consent from a parent or guardian.

This research takes into account these factors listed in order to ensure that all ethical considerations are complied with. As my research focused on a selected financial institution, I did not interview any organisations or employees of organisations who are competitors of the organisation in this study. Consent was received from the organisation to conduct the research, and the name of the organisation is not disclosed in the research.

#### **4.13 Summary**

This chapter described the methodology that provided a breakdown of the research study's design and methodology applied to achieve the research questions and objectives. The research study's design and methodology further explained the validity and reliability of the quantitative and qualitative approach.

The research study's population and sampling were outlined in the design of the questionnaire and semi-structured interviews. The ethical considerations explained were considered in relation to the aim and purpose of the research study. The pilot testing, distribution and collection of the questionnaire and conducting of interviews were reported and are aligned to research practices. The data presentation and analysis are explained in Chapters 5 and 6.

## CHAPTER FIVE: DATA PRESENTATION AND ANALYSIS (a)

### 5.1 Introduction

This chapter presents the results and discusses the findings obtained from the questionnaires in this study. This chapter starts with covering reliability testing and factor analysis for the overall study. This is followed by the results and descriptive statistics presented in the form of graphs, cross-tabulations and other figures for the quantitative data that was collected. Furthermore, inferential techniques which include the use of correlations and chi square test values are shown and interpreted using p-values. The data collected from the research study's questionnaire was analysed and presented by using descriptive statistics to quantify the data in line with the research study's main objective. Lastly, hypothesis testing was used in the analysis.

### 5.2 Reliability testing

The two most important aspects of precision are reliability and validity. Reliability is computed by taking several measurements on the same subjects. Cronbach's alpha coefficient was applied to all statements consisting of Likert Scale responses in the questionnaire. According to Chigamba and Fatoki (2011: 66-70), the Cronbach alpha coefficient is used to test the reliability of the scales used by the researcher with the alpha coefficient ranging from 0 to 1 with the higher score indicating a higher degree of reliability of the scale. Cooper and Schindler (2003) state that a reliability coefficient of 0.70 or higher is considered as the acceptable reliability coefficient.

**Table 5.1: Cronbach's alpha coefficient for the quantitative measuring instrument**

Section		Number of Items	Cronbach's Alpha
B	Breaching of data in a financial institution	15 of 15	0.777
C	Information management mitigation in a financial institution	13 of 13	0.788
D	Information management preparedness in a financial institution	7 of 7	0.787
E	Information management systems in a financial institution	12 of 12	0.780
F	Risk response and recovery in a financial institution	11 of 11	0.800
<b>OVERALL</b>		<b>58 of 58</b>	<b>0.847</b>

The reliability scores for all sections exceeded the recommended Cronbach's alpha value of 0.700. An overall Cronbach's alpha value of 0.847 was achieved in this study. This indicates a degree of acceptable, consistent scoring for the different sections of the research. No questions were, thus, omitted from the analysis.

### 5.3 Factor analysis

As highlighted in Chapter 4, factor analysis is a statistical technique whose main goal is data reduction. A typical use of factor analysis is in survey research where a researcher wishes to represent a number of questions with a small number of hypothetical factors (Refer to Appendix E for full results on factor analysis).

**Table 5.2: KMO and Bartlett's test**

Section		Kaiser-Meyer-Olkin Measure of Sampling Adequacy	Bartlett's Test of Sphericity		
			Approx. Chi-Square	df	Sig.
B	Breaching of data in a financial institution	0.783	534.613	105	0.000
C	Information management mitigation in a financial institution	0.780	366.723	78	0.000
D	Information management preparedness in a financial institution	0.829	168.332	21	0.000
E	Information management systems in a financial institution	0.831	342.859	66	0.000
F	Risk response and recovery in a financial institution	0.771	315.878	55	0.000

The requirement is that Kaiser-Meyer-Olkin Measure of Sampling Adequacy should be greater than 0.500 and Bartlett's Test of Sphericity less than 0.05. In all instances, the conditions were satisfied in this research as shown by the sig values being 0.000 which allows for the factor analysis procedure on the questionnaire data.

A typical use of factor analysis is in survey research, where a researcher wishes to represent a number of questions with a small number of hypothetical factors. This test indicates there was a relationship amongst these dimensions at 0.000, which indicates that the majority of respondents agreed with these statements. This is further discussed and analysed with the various sections to follow in this chapter.

### 5.4 Research findings and analysis

Even though the majority of respondents agreed, gaps were also found, which necessitates interventions or control measures to be implemented by decision-makers of the institution.

**Table 5.3: Breaching of data in a financial institution**

Breaching of data in a financial institution	Disagree	Undecided	Agree
I ensure that I do not breach confidential information	1%	3%	96%
I ensure that I secure organisational personal information	1%	3%	96%
I make sure that I don't breach security information	1%	1%	98%
I'm not associated in fraudulent activities	1%	0%	99%
My activities are aligned to government regulations	1%	17%	82%
There are no occurrences of information breaches	6%	27%	67%

Data breaches has a positive impact	67%	17%	16%
Customers are not concerned about information management	58%	25%	17%
Breaching of information is assessed	7%	29%	64%
Employees are trained on information security policies	6%	20%	74%
Experienced employees are more compliant on security policies	9%	27%	64%
Employees keep customer information confidential	5%	23%	72%
Employees are held accountable for breaching customer data	9%	15%	76%
Data breaches do not affect its economic condition	61%	33%	6%
Data breaches only occur accidentally	69%	21%	10%

Table 5.3 indicates that the majority of research participants were in agreement with the sub-dimensions on the breaching of data in a financial institution with the exception of only two disagreements on the fact that data breaches have a positive impact and that customers are not concerned about information management. The research findings in Table 5.3 reveal a disproportionately high percentage on the agreement that employees do not breach confidential information and secure personal information (96%), respectively; security information (98%); not associated with fraudulent activities (99%) and aligned to government regulations (82%). This was followed by the research participants who indicated that employees are accountable (76%); training employees on security policies (74%); and keeping of customer information confidentially (72%). The majority of the research participants were in disagreement regarding the fact that data breaches has a positive impact (67%) and that customers are not concerned about information management (58%). Furthermore, Table 5.3 reflects 61% of the research participants were against the fact that data breaches do not affect its economic condition and that it occurs accidentally (69%).

The high percentage of agreements to the first 6 statements could indicate that employees take care in protecting information. There are 99% of respondents who stated that they are not involved in fraudulent activities at the institution, this is aligned with statements 'I ensure that I do not breach confidential information', 'I ensure that I secure organisational personal information' and 'I make sure that I don't breach security information'; this indicates that employees associate breaching of information as fraud and, therefore, keep information safe. A high percentage of respondents positively agreed that their activities are aligned to government regulations (82%) while 17% were undecided. Therefore, almost 1/5 employees either moderately responded by selecting 'undecided' or are not sure if their activities are or are not aligned to government regulations. This indicates that these 1/5 employees may not be aware of the government regulations that are impacted on their roles.

The table also showed that 66% of respondents stated that there are no occurrences of information breaches at the organisation. There are 27% who were undecided while 6% disagreed and stated

that there are instances of information breaches at the organisation. Therefore, a minority of the respondents (6%) stated that they know there are data breaches while 67% believe that there are no data breaches. Over a ¼ of respondents are undecided - which could indicate they are not certain if there are data breaches or not that occur at the institution. Moreover, 1/3 respondents either agreed or were undecided that data breaches has a positive impact; 17% were undecided and 16% agreed. This means that only 67% of respondents stated that data breaches do not have a positive impact. It indicates that there is a considerable percentage of employees who are explicitly of the opinion that data breaches are not negative to the organisation. There are 58% of respondents who disagreed with the statement that customers are not concerned about information management while a ¼ of respondents were undecided, which indicates that they are not sure what customer expectations are in relation to information management. There are 17% of respondents who were of the opinion that customers are not concerned about information management and 64% of respondents who agree that breaching of information is assessed at the institution. More than 1/3 of respondents, therefore, either do not know if breaching of information is assessed at the institution or are of the opinion that it is not. This indicates that there is a considerable amount of employees who are not familiar with data breaching processes or company policy on data breaching.

There are 26% of respondents who stated that employees are not trained or do not know if employees are trained on information security policies. A high percentage (74%) of respondents agreed that employees do receive training on information security policies. This, however, indicates that there is no a uniform approach to information security policies training at the institution. There are 64% of respondents who agreed to the statement that experienced employees are more compliant on security policies while 27% of respondents either moderately responded by selecting 'undecided' or said the employees are not sure. This indicates that a fair amount of respondents are of the opinion that employees who have been in employ for longer are less likely to digress from security policies within the organisation.

In addition, 72% of respondents agreed with the statement that employees keep customer information confidential. A small percentage (5%) of respondents disagreed with the statement. Almost ¼ respondents were undecided. This indicates that the ¼ employees may not always be keeping customer information confidential or may not know what keeping customer information confidential entails while the majority of employees undertake to the responsibility of keeping customer information confidential. More than 3/4 of respondents agreed that employees are held accountable for breaching customer data, and 15% responded moderately by selecting 'undecided' or 'not sure'. This indicates that most employees are aware what the repercussion are for breaching customer data or that employees are aware of the responsibility that they have when dealing with customer data. Close to



40% of respondents were either undecided or agreed (33% undecided, 6% agree) that data breaches do not affect the economic condition of the organisation. This indicates that there could be a lack of understanding of what the negative impact of data breaches could be on the organisation. There are 69% of the respondents who disagreed to the statement that data breaches only occur accidentally, and 10% of the respondents agreed to the statement while 21% were undecided. The majority of respondents were of the opinion that that data breaches are an accident, which indicates that these respondents could perceive that individuals are knowingly breaching data within the organisation.

Of the 15 statements that comprise this section, 11 show (significantly) higher levels of agreement whilst 4 show greater levels of disagreement. The negative statements concentrated on perceived customer responses, economic impact and nature of occurrence of data breaches. The matrix table on factor analysis on this section is displayed in Appendix E, in the section Rotated component matrix for breaching of data in a financial institution. Factor analysis shows that the first 6 statements form a sub-theme ('I ensure that I do not breach confidential information', 'I ensure that I secure organisational personal information', 'I make sure that I don't breach security information', 'I'm not associated in fraudulent activities', 'My activities are aligned to government regulations' and 'There are no occurrences of information breaches'). This sub-theme falls under the grouping of employees' Personal Attitudes to Data Breaches.

There are high levels of agreement relation to Personal Attitudes to Data Breaches. This could indicate that respondents have an understanding of the consequences of a data breach and are vigilant in terms of the precautions they take. Factor analysis shows that statements 'Data breaches has a positive impact', 'Customers are not concerned about information management', 'Experienced employees are more compliant on security policies', 'Data breaches do not affect its economic condition' and 'Data breaches only occur accidentally' form a sub-theme of Impact and Reasons of Data Breaches. There are mainly higher levels of disagreement to the sub-theme of Impact and Reasons of Data Breaches. Factor analysis shows that statements 'Breaching of information is assessed', 'Employees are trained on information security policies', 'Employees keep customer information confidential', and 'Employees are held accountable for breaching customer data to form a sub-theme of Employee Knowledge and Assessment of Data Breaches. There are higher levels of agreement on Employee Knowledge and Assessment of Data Breaches. This could indicate that respondents have knowledge of what a data breach is and how to assess if data breaches can occur.

A chi-square test was done on breaching of data in a financial institution and indicates that the scoring patterns are somewhat similar, proportionally. This is confirmed by the chi-square p-values ( $p < 0.05$ ) which confirms that the differences observed per option per statement were significant. The sig.

values (p-values) or level of significance are less than 0.05, it implies that the distributions were not similar, that is, the differences between the way respondents scored (agree, undecided, disagree) were significant. The table is displayed in Appendix F, section Chi-square test of breaching of data in a financial institution.

**Table 5.4: Information management mitigation in a financial institution**

Information management mitigation in a financial institution	Disagree	Undecided	Agree
Information management security policies are in place	3%	6%	91%
Information management programmes are in place to educate employees	8%	20%	72%
There is low risk of information breaches	26%	43%	31%
Information is protected from the moment it is created until the end of its cycle	27%	35%	38%
I have access to customer information that is not a necessity to perform my job	52%	10%	38%
I have attended information management training which is beneficial to me	49%	14%	37%
Information management risks are managed well	10%	38%	52%
Risk assessments are done in order to quantify threats	6%	42%	52%
Management plays an important role to promote information security	11%	17%	72%
Money is spent to mitigate data breaches	8%	33%	59%
Information security is part of my organisational culture	10%	23%	67%
There are awareness campaigns on information security	17%	20%	63%
Employees' knowledge is regularly tested on information security policies and procedures	37%	26%	37%

Table 5.4 indicates that the majority of research participants were in agreement with eight sub-dimensions on information management mitigation in a financial institution, with the exception of one on the item 'I have access to customer information that is not a necessity to perform my job while four statements did not have an outright majority selection by participants'. The research findings in Table 5.4 reveal that of the agreements, there was no disproportionately high percentage on the agreements except for information management security policies being in place (91%). Further majority agreements were for statements 'information management programmes are in place to educate employees' (72%); 'management plays an important role to promote information security' (72%); 'information security is part of my organisational culture' (67%); 'there are awareness campaigns on information security' (63%); 'money is spent to mitigate data breaches' (59%); and 'both risk assessments are done in order to quantify threats' and 'information management risks are managed well' (52%). The majority of the research participants were in disagreement regarding the fact statement 'I have access to customer information that is not a necessity to perform my job' (52%). Statements that did not have an outright majority selection are: information is protected from the moment it is created until the end of its cycle (agree 38%, undecided 35%, disagree 27%); I have attended information management training which is beneficial to me (agree 37%, undecided 14%, disagree 49%); employees' knowledge is regularly tested on information security policies and

procedures (agree 37%, undecided 26%, disagree 37%); and there is low risk of information breaches (agree 31%, undecided 43%, disagree 26%).

A significantly high number of respondents (91%) agreed to the statement that there are information management security policies at the institution while 72% of respondents agree to the statement that information management programmes are in place to educate employees. This could indicate that employees know that there are policies at the organisation in relation to information management. However, the same amount of employees may not believe that programmes are in place at the organisation to educate employees on these policies. There is a high degree of variation in response to statements: 'There is low risk of information breaches' and 'Information is protected from the moment it is created until the end of its cycle'. In addition, 43% of respondents were undecided if there is a low risk of information breaches at the institution while 31% agreed to the statement and 26% disagreed. There are 38% of respondents who agreed and 27% disagreed (35% undecided) to the statement that information is protected from the moment it is created until the end of its cycle. This indicates that employees possibly do not understand what the risk of information breaches are and that this sub-theme of Information Protection is perceived differently by employees or that there is no standard level of information protection across all employees at the organisation. Just over ½ of respondents disagreed to the statement that they have access to information that is not a necessity to perform their job while 38% agreed to this statement. This indicates that access to the appropriate information required to perform a role is not managed in a standard manner across the organisation.

Almost ½ of the respondents disagreed to the statement that they have attended information management training that is beneficial to them. There are 37% who agreed to the statement and 14% were undecided. This indicates that there is a potential lack of positive training in relation to information management at the organisation. Just over ½ of respondents agreed to statements 'Information management risks are managed well' and 'Risk assessments are done in order to quantify threats'. There are 38% who were undecided on statement 'Information management risks are managed well' and 42% were undecided on statement 'Risk assessments are done in order to quantify threats'. This indicates that although half of the respondents positively agreed, there is a substantial percentage of employees who may not understand the process of information management in the organisation and also possibly what their role is when it comes to the concept of information management. The majority of respondents (72%) agreed with the statement that management plays an important role to promote information security while 11% disagreed with the statement. This indicates that employees could use clear direction from management in relation to information security and more specifically, how to handle and protect information. Just under 60% of respondents agree to the statement that money is spent to mitigate data breaches whilst 1/3

moderately responded by selecting undecided and 8% disagreed to the statement. Therefore, although most employees believe that money is being spent to combat data breaches at the organisation, there is still a fair amount of employees that are not sure what monetary resources are being put into mitigating data breaches, which could indicate that these employees do not understand the overall organisational strategy and plan for data breaches.

There are 67% of respondents who positively agreed to the statement 'Information security is part of my organisational culture' and 63% positively agreed to statement 'There are awareness campaigns on information security'. Therefore, approximately 2/3 employees believe that information security is part of the culture of the organisation and that the organisation creates awareness campaigns as an enabler to create this culture. The majority of employees positively agreed; however, there were still approximately 1/3 employees who believe that they are not sure if there are awareness campaigns on information security and if information security is not part of the DNA of the organisation. This indicates that there is a positive attempt by the organisation to promote information security, but it may not be reaching all employees. In addition, 37% of respondents both agreed and disagreed that employees' knowledge is regularly tested on information policies and procedures while 26% were undecided. This indicates that there may not be a standard set of practises applied across the organisation and also that employees are possibly not getting the same degree of exposure to policies and procedures relating to information security.

The matrix table on factor analysis on this section is displayed in Appendix E, in the section Rotated Component Matrix for information management in a financial institution. Factor analysis shows that statements 'Information management programmes are in place to educate employees', 'Information is protected from the moment it is created until the end of its cycle', 'There are awareness campaigns on information security' and 'Employees' knowledge is regularly tested on information security policies and procedures' are related whereby the sub-theme is of Employee Knowledge and Awareness of Information Management. Factor analysis shows that statements 'There is low risk of information breaches', 'Risk assessments are done in order to quantify threats', 'Money is spent to mitigate data breaches' and 'Information security is part of my organisational culture' form a sub-theme of Data Breaching Avoidance. Factor analysis shows that statements 'Information management security policies are in place', 'I have attended information management training which is beneficial to me', 'Information management risks are managed well' and 'Management plays an important role to promote information security' are related whereby the sub-theme is of Management Input to Information Management Mitigation.

Chi-square were done on the dimension information management mitigation in a financial institution to determine whether the scoring patterns per statement were significantly different per option. Most of the scoring patterns are somewhat similar, proportionally. This is confirmed by the chi-square p-values ( $p < 0.05$ ) which confirm that the differences observed per option per statement were significant. This applies to statements 'Information management security policies are in place', 'Information management programmes are in place to educate employees', 'I have access to customer information that is not a necessity to perform my job', 'I have attended information management training which is beneficial to me', 'Information management risks are managed well', 'Risk assessments are done in order to quantify threats', 'Management plays an important role to promote information security', 'Money is spent to mitigate data breaches', 'Information security is part of my organisational culture' and 'There are awareness campaigns on information security'. Statements 'There is low risk of information breaches', 'Information is protected from the moment it is created until the end of its cycle' and 'Employees' knowledge is regularly tested on information security policies and procedures' did not have significant differences in opinions. This is confirmed by the chi-square p-values being 0.146 for statement 'There is low risk of information breaches', 0.459 for statement 'Information is protected from the moment it is created until the end of its cycle' and 0.368 for statement 'Employees' knowledge is regularly tested on information security policies and procedures'. This is displayed in Appendix F, section Chi-square test of information management mitigation in a financial institution.

**Table 5.5: Information management preparedness in a financial institution**

<b>Information management preparedness in a financial institution</b>	<b>Disagree</b>	<b>Undecided</b>	<b>Agree</b>
I am aware of government regulations and procedures on information management	14%	17%	69%
Employees are the strongest link in information security	7%	15%	78%
If data breaches do occur there is a set procedures in place that I will follow	9%	23%	68%
Information management security is part of my institutional culture	7%	24%	69%
Policies on information management are clear	10%	28%	62%
There are disciplinary measures in place to address employee negligence on information management	7%	16%	77%
Information security forms part of the annual organisations budgeting	9%	53%	38%

Table 5.5 indicates that the majority of research participants were in agreement with the sub-dimensions on information management preparedness in a financial institution with the exception of only one statement where the majority of participants were undecided on the fact that information security forms part of the annual organisation's budget. The research findings in Table 5.5 reveal that the majority agreements of 'employees are the strongest link in information security' (78%); 'there are

disciplinary measures in place to address employee negligence on information management (77%); 'I am aware of government regulations and procedures on information management' (69%); 'information management security is part of my institutional culture' (69%); 'if data breaches do occur there is a set procedures in place that I will follow' (68%); and 'policies on information management are clear' (62%). The majority of participants were undecided to the statement 'information security forms part of the annual organisations budgeting' (53%).

Statements 'I am aware of government regulations and procedures on information management' to 'There are disciplinary measures in place to address employee negligence on information management' all show a higher level of agreement with respondents disagreeing to these statements making up the minority of responders. Therefore, where respondents moderately responded, the undecided option was the second highest option chosen which ranged between 16% and 28% for these statements. This indicates that employees are aware of preparedness plans to information management and believe that employees are the strongest link to information security. More than ½ of the respondents selected the undecided option to the statement that information security forms part of the annual organisations budget, 38% agreed while 9% disagreed. This indicates that there may not be large amounts of monetary investments spent or set aside by the organisation for information security.

The matrix table on factor analysis on this section is displayed in Appendix E, section Rotated component matrix for information management preparedness in a financial institution. Factor analysis shows that there is a relation between the last 5 statements ('If data breaches do occur there is a set procedures in place that I will follow', 'Information management security is part of my institutional culture', 'Policies on information management are clear', 'There are disciplinary measures in place to address employee negligence on information management' and 'Information security forms part of the annual organisations budgeting'). This forms the sub-theme of Organisational Policies, Procedures and Planning of Information Management. Factor analysis shows that statements 'I am aware of government regulations and procedures on information management' and 'Employees are the strongest link in information security' form a sub-theme. There are higher levels of agreement to this sub-theme of Employee Contribution and Awareness of Governmental Regulations on Information Management. This could indicate that respondents have an understanding of the role they play to information management and how this impacts governmental regulations and procedures.

The chi-square test was done on information management preparedness in a financial institution. All of the scoring differences are significant per statement. This is confirmed by the chi-square p-values ( $p < 0.05$ ) which confirm that the differences observed per option per statement were significant. This

is displayed in Appendix F, section Chi-square test of information management preparedness in a financial institution.

**Table 5.6: Information management systems in a financial institution**

<b>Information management systems in a financial institution</b>	<b>Disagree</b>	<b>Undecided</b>	<b>Agree</b>
Technology based solutions are all that is required to ensure information security	64%	22%	14%
Without IT systems we cannot control information management	16%	10%	74%
The software systems I use have strict access control to customer information	16%	14%	70%
The IT systems are aligned with the requirements of protecting customer information	7%	20%	73%
Data protection and security protection controls are in place on computers	3%	11%	86%
Employees have access to pass customer information to a third party. E.g. via email	25%	12%	63%
All interactions with customers are recorded on an IT system	6%	27%	67%
The IT area is well informed of necessities related to privacy regulation and policies	6%	31%	63%
The standard of information security systems are assessed against international accepted rules and practises	3%	48%	49%
Employees are required to demonstrate to consumers their level of compliance in relation to information security guidelines	12%	37%	51%
All business stakeholders are involved when implementing IT systems	23%	41%	36%
Information systems are becoming more exposed to risk and breaches	17%	40%	43%

Table 5.6 indicates that the majority of research participants were in agreement with the sub-dimensions on the information management systems in a financial institution, with the exception of one disagreement on the fact that technology based solutions are all that is required to ensure information security; three statements did not have a majority selection. The research findings in Table 5.6 reveal a disproportionately high percentage on the agreement that data protection and security protection controls are in place on computers (86%).

There are further majority agreements to: without IT systems we cannot control information management (74%); the IT systems are aligned with the requirements of protecting customer information (73%); the software systems I use have strict access control to customer information (70%); all interactions with customers are recorded on an IT system (67%); the IT area is well informed of necessities related to privacy regulation and policies (63%); employees have access to pass customer information to a third party. E.g. via email (63%); and employees are required to demonstrate to consumers their level of compliance in relation to information security guidelines (51%). The majority of the research participants were in disagreement regarding the fact that technology based solutions are all that is required to ensure information security (64%). Statements that did not have an outright majority selection are: the standard of information security systems are assessed against international accepted rules and practises (agree 49%, undecided 48%, disagree 3%); all business stakeholders are involved when implementing IT systems (agree 36%, undecided

41%, disagree 23%); and information systems are becoming more exposed to risk and breaches (agree 43%, undecided 40%, disagree 17%).

Just under 2/3 respondents disagreed to the statement that technology based solutions are all that is required to ensure information security. Therefore, just over 1/3 respondents agreed or were undecided (14% agreed and 22% undecided). This indicates that most employees possibly understand their role as an employee to protect organisation information; however, there is still a fair amount of employees that may not understand their role as an employee to protect organisational information and may believe that it is the sole responsibility of technology to protect information.

Nearly ¾ respondents believe that without IT, systems information management cannot be controlled. This could indicate that employees believe that IT systems and IT infrastructure plays an important role in the organisation's plan to control and secure information, and there may be an expectation by employees that these IT systems are of a high standard. There are 70% of respondents who agreed to the statement that the software systems that they use have strict access control to customer information, and 16% of respondents disagreed to the statement. This indicates that there is no standard set of controls applied to all software systems across the organisation. A high percentage of respondents (73%) agree to the statement that the IT systems are aligned with the requirements of protecting customer information. There is, therefore, still a fair amount of respondents (more than ¼) who perceive that their IT systems are not aligned to these requirements mentioned or are undecided, which could indicate that these employees do not know what these requirements entail.

There are 86% of respondents who believe that data protection and security protection controls are in place in computers, and 3% disagreed to the statement. This indicates that employees may have a limited chance of breaching information from a system perspective. There are 63% of respondents who agreed to the statement that they have permission to pass customer information to a third party e.g. via email while ¼ respondents disagreed. This could indicate that certain employees require this permission or access to perform their job and some may not. This also indicates that there may be a high potential to breach data in this regard. Findings revealed that 2/3 of respondents believe that all interactions with customers are recorded on an IT system while 27% were undecided. This could indicate that employees who deal with customers are aware of what the systems cater for in relation to storing customer interactions while there may be employees who do not deal directly with customers and therefore may not know what systems are in place to record customer interactions. There are 63% of respondents who agreed to the statement that the IT area is well informed of necessities related to privacy regulation and policies; 31% moderately responded by selecting undecided while 6% disagreed to the statement. This indicates that most employees are confident in



the knowledge that the IT area holds in relation to privacy regulation and policies while the number of respondents who selected 'undecided' indicates that there are also a fair amount of employees who may not be knowledgeable of IT plans and strategy on information management regulation and policies.

There are 49% of respondents who agreed and 48% disagreed to the statement that the standard of information security systems are assessed against international accepted rules and practises. Therefore, almost an equal split of employees are aware of the standard of the IT systems at the organisation (agreed) while the other half are not aware of the standard of the IT systems, which indicates that there may not be a standard awareness on this driven by the organisation. There are 51% of respondents who agreed to the statement employees are required to demonstrate to consumers their level of compliance in relation to information security guidelines (12% disagreed and 37% undecided). This, again, speaks to the fact that there is a possibly that no standard practise applied across the organisation or it could indicate that not all employees deal directly with customers.

There were split responses to the statement that all business stakeholders are involved when implementing IT systems; 36% agreed, 23% disagreed, and 41% undecided. This indicates that most employees may believe that they are not involved when implementing IT systems. There are 43% who agreed to the statement 'Information systems are becoming more exposed to risk and breaches'. Therefore, over half of respondents believe that information systems are becoming more exposed to risk and breaches. This indicates that a large number of employees may not be aware of the risks which result from data breaches or how potential risks affect the systems that employees work on.

The matrix table on factor analysis on this section is displayed by Appendix E, section Rortated component matrix for information management systems in a financial institution. Factor analysis shows that there is a relationship between statements 'Without IT systems we cannot control information management', 'The software systems I use have strict access control to customer information', 'The IT systems are aligned with the requirements of protecting customer information', 'Data protection and security protection controls are in place on computers', 'All interactions with customers are recorded on an IT system', 'The IT area is well informed of necessities related to privacy regulation and policies', 'The standard of information security systems are assessed against international accepted rules and practises', 'Employees are required to demonstrate to consumers their level of compliance in relation to information security guidelines' and 'All business stakeholders are involved when implementing IT systems'. This creates the sub-theme of IT Systems Security and Control. The majority of the statement had higher levels of agreement than disagreement.

Chi-square tests were done on the dimension information management systems in a financial institution to determine whether the scoring patterns per statement were significantly different per option. Most of the scoring patterns are somewhat similar, proportionally. This is confirmed by the chi-square p-values ( $p < 0.05$ ) which confirm that the differences observed per option per statement were significant. This applies to statements ‘Technology based solutions are all that is required to ensure information security’, ‘Without IT systems we cannot control information management’, ‘The software systems I use have strict access control to customer information’, ‘The IT systems are aligned with the requirements of protecting customer information’, ‘Data protection and security protection controls are in place on computers’, ‘Employees have access to pass customer information to a third party. e.g. via email’, ‘All interactions with customers are recorded on an IT system’, ‘The IT area is well informed of necessities related to privacy regulation and policies’, ‘The standard of information security systems are assessed against international accepted rules and practises’, ‘Employees are required to demonstrate to consumers their level of compliance in relation to information security guidelines’ and ‘Information systems are becoming more exposed to risk and breaches’. The statement ‘All business stakeholders are involved when implementing IT systems’ did not have significant differences in opinions. This is confirmed by the chi-square p-values being 0.146 for the statement. This is displayed in Appendix F, section Chi-square test of information management systems in a financial institution.

**Table 5.7: Risk response and recovery in a financial institution**

<b>Risk response and recovery in a financial institution</b>	<b>Disagree</b>	<b>Undecided</b>	<b>Agree</b>
Information risk management is not important	96%	1%	3%
Risk management does not need to form part of a business strategy	95%	4%	1%
The requirement for risk management is on the decrease	69%	27%	4%
Regulatory risks should not form part of the institution’s risk plan	90%	9%	1%
There are no controls in place to react to information management risks	72%	22%	6%
We do not respond well to risks on information management	69%	21%	10%
There are no contingency plans in place to deal with risks on information management	64%	31%	5%
Information is not securely backed up in the event it should be lost	65%	26%	9%
I am not able to identify information risks	72%	15%	13%
I reactively respond to information risks	33%	30%	37%
There are instances when I do not get notifications on information risks	35%	26%	39%

Table 5.7 indicates that the majority of research participants were in disagreement with the sub-dimensions on the breaching of data in a financial institution while two statements did not have a majority selection. Table 5.7 further reveals a disproportionately high percentages on the disagreement of information risk management not being important (96%); ‘risk management does not need to form part of a business strategy’ (95%); and ‘regulatory risks should not form part of the

institution's risk plan' (90%). Further majority disagreements were for: there are no controls in place to react to information management risks (72%); I am not able to identify information risks (72%); the requirement for risk management is on the decrease (69%); we do not respond well to risks on information management (69%); information is not securely backed up in the event it should be lost (65%); and there are no contingency plans in place to deal with risks on information management (64%). Statements that did not have an outright majority selection are: I reactively respond to information risks (agree 37%, undecided 30%, disagree 33%); and there are instances when I do not get notifications on information risks (agree 39%, undecided 26%, disagree 35%).

Most respondents (96% and 95%) disagreed to the statements that information risk management is not important and that risk management does not need to form part of a business strategy. This indicates there is a high degree of understanding of the magnitude of information risk management by employees and that employees believe that information risk management requires a proper plan and strategy to proactively respond to potential data breaches. There are 69% of respondents who disagreed to the statement that the requirement for risk management is on the decrease. More than ¼ of respondents, however, moderately responded by choosing the 'undecided' option. This could indicate that although most of respondents believe that risk management is important, as highlighted in statements 'Information risk management is not important' and 'Risk management does not need to form part of a business strategy'. There is, however, a fair amount of employees who seemed unaware of the frequency of information management breaches and were therefore not aware if the requirement for risk management is on the decrease. Moreover, 90% of respondents believe that regulatory risks should form part of the institution's risk plan. This indicates that employees could believe that governmental policies should tie in with organisational policies on information management; therefore, the organisation requires a plan and strategy in response to potential information breaches.

There are 72% of respondents who disagreed to the statement that there are no controls in place to react to information management risks, 69% of respondents disagreed to the statement: 'we do not respond well to risks on information management' while 64% of respondents disagreed to the statement that there are no contingency plans in place to deal with risks on information management. Therefore, approximately 1/3 respondents either agree or are undecided. This could indicate that not all employees are knowledgeable and aware of response strategies for information management and that there are no standard tools used for all employees to get them equipped to deal with information management risks.

There are 65% who disagreed, 9% agreed and 26% of respondents were undecided to the statement that information is not securely backed up in the event it should be lost. The majority of respondents, therefore, believe that there is a recovery strategy and plan should information be lost; ¼ of respondents may not be aware of this strategy and plan, which again indicates that there may not be a standard mechanism of communicating these strategies to all employees or that certain employees do not deal with this type of IT related backup procedures and are, therefore, not aware of this recovery strategy.

A high number of respondents (72%) disagree to the statement: 'I am not able to identify information risks'. This could indicate that the majority of employees are aware of what is expected of them in response to information management risks and breaches. There is still, however, a fair amount of more than ¼, of employees that may not be aware of what is expected of them in relation to this category. The responses to statements 'I reactively respond to information risks' and 'There are instances when I do not get notifications on information risks' were spread across the Likert scale. There were similar percentages recorded in the way that responders answered these statements. Moreover, 37% and 39% agreed, 33% and 35% disagreed while 30% and 26% were undecided. This indicates that the way employees respond to information risks varies across employees in the organisation whereby some employees are reactive while others are proactive. In addition, there may also be an indication that not all employees are notified on information risks, and this may, therefore, somewhat impact the way they respond.

The matrix table on factor analysis on this section is displayed in Appendix E, section Rotated component matrix for risk response and recovery in a financial institution. Factor analysis shows that there is a relationship between statements: 'There are no controls in place to react to information management risks', 'We do not respond well to risks on information management', 'There are no contingency plans in place to deal with risks on information management', 'Information is not securely backed up in the event it should be lost' and 'There are instances when I do not get notifications on information risks'. This creates the sub-theme Information Risk Planning and Controlling. Factor analysis shows that statements: 'Information risk management is not important', 'Risk management does not need to form part of a business strategy' and 'Regulatory risks should not form part of the institution's risk plan' create the sub-theme Employee Perception to Information Risk. Factor analysis shows that there is a relationship between statements: 'I am not able to identify information risks' and 'I reactively respond to information risks'. This creates the sub-theme Information Risk Identification and Response.

Chi-square tests were done on the dimension information management preparedness in a financial institution to determine whether the scoring patterns per statement were significantly different per option. Most of the scoring patterns are somewhat similar, proportionally. This is confirmed by the chi-square p-values ( $p < 0.05$ ), which confirms that the differences observed per option per statement were significant. This applies to statements: 'Information risk management is not important', 'Risk management does not need to form part of a business strategy', 'The requirement for risk management is on the decrease', 'Regulatory risks should not form part of the institution's risk plan', 'There are no controls in place to react to information management risks', 'We do not respond well to risks on information management', 'There are no contingency plans in place to deal with risks on information management', 'Information is not securely backed up in the event it should be lost' and 'I am not able to identify information risks'. Statements 'I reactively respond to information risks' and 'There are instances when I do not get notifications on information risks' did not have significant differences in opinions. This is confirmed by the chi-square p-values being 0.717 for statement: 'I reactively respond to information risks' and 0.317 for statement: 'There are instances when I do not get notifications on information risks'. This is displayed in Appendix F, section Chi-square test of risk response and recovery in a financial institution.

## **5.5 Hypothesis testing**

The traditional approach to reporting a result requires a statement of statistical significance. A p-value is generated from a test statistic, and a significant result is indicated with ' $p < 0.05$ '.

A second Chi square test was performed to determine whether there was a statistically significant relationship between the variables (rows vs columns or biographical data vs Likert scale responses). The null hypothesis states that there is no association between the two. The alternate hypothesis indicates that there is an association (Refer to Appendix C for full results of hypothesis testing). The hypothesis testing is discussed below.

The p-value between: 'I ensure that I do not breach confidential information' and 'Highest level of education completed' is 0.024. This means that there is a significant relationship between the variables, that is, the education level of the respondent did play a significant role in terms of how respondents viewed breach of confidential information. The p-value between 'I ensure that I do not breach confidential information' and 'Area of specialisation' is 0.010. This means that there is a significant relationship between the variables, that is, the area of specialisation of the respondent did play a significant role in terms of how respondents viewed breach of confidential information. The p-value between 'I ensure that I secure organisational personal information' and 'Highest level of education completed' is 0.024. This means that there is a significant relationship between the variables. That is, the education level of the respondent did play a significant role in terms of how

respondents viewed security of organisational information. The p-value between 'I ensure that I secure organisational personal information' and 'Area of specialisation' is 0.010. This means that there is a significant relationship between the variables. That is, the area of specialisation of the respondent did play a significant role in terms of how respondents viewed security of organisational information. The p-value between 'I make sure that I don't breach security information' and 'Highest level of education completed' is 0.021. This means that there is a significant relationship between the variables, that is, the education level of the respondent did play a significant role in terms of how respondents viewed breaching of secured information. The p-value between 'I make sure that I don't breach security information' and 'Area of specialisation' is 0.042. This means that there is a significant relationship between the variables, that is, the area of specialisation of the respondent did play a significant role in terms of how respondents viewed breaching of secured information. The p-value between 'I'm not associated in fraudulent activities' and 'Highest level of education completed' is 0.004. This means that there is a significant relationship between the variables, that is, the education level of the respondent did play a significant role in terms of how respondents viewed association to fraud.

The p-value between 'I'm not associated in fraudulent activities' and 'Area of specialisation' is 0.007. This means that there is a significant relationship between the variables, that is, the area of specialisation of the respondent did play a significant role in terms of how respondents viewed association to fraud. The p-value between 'My activities are aligned to government regulations' and 'Highest level of education completed' is 0.009. This means that there is a significant relationship between the variables, that is, the education level of the respondent did play a significant role in terms of how respondents viewed their activities alignment to government regulations. The p-value between 'My activities are aligned to government regulations' and 'Area of specialisation' is 0.015. This means that there is a significant relationship between the variables, that is, the area of specialisation of the respondent did play a significant role in terms of how respondents viewed their activities alignment to government regulations. The p-value between 'There are no occurrences of information breaches' and 'Age' is 0.004. This means that there is a significant relationship between the variables, that is, the age of the respondent did play a significant role in terms of how respondents viewed the occurrences of information breaches. The p-value between 'There are no occurrences of information breaches' and 'How long have you been in this position at the company' is 0.007. This means that there is a significant relationship between the variables, that is, the length of service of the respondent did play a significant role in terms of how respondents viewed the occurrences of information breaches.

The p-value between 'Employees keep customer information confidential' and 'Age' is 0.042. This means that there is a significant relationship between the variables, that is, the age of the respondent did play a significant role in terms of how respondents viewed confidentiality customer information. The p-value between 'Employees are held accountable for breaching customer data' and 'Age' is 0.025. This means that there is a significant relationship between the variables, that is, the age of the respondent did play a significant role in terms of how respondents viewed accountability for breaching customer data. The p-value between 'Data breaches do not affect its economic condition' and 'Highest level of education completed' is 0.037. This means that there is a significant relationship between the variables, that is, the education level of the respondent did play a significant role in terms of how respondents viewed the economic effect of data breaches.

The p-value between 'Data breaches do not affect its economic condition' and 'Staffing level' is 0.009. This means that there is a significant relationship between the variables, that is, the staffing level of the respondent did play a significant role in terms of how respondents viewed the economic effect of data breaches. The p-value between 'Information management programmes are in place to educate employees' and 'Age' is 0.007. This means that there is a significant relationship between the variables, that is, the age of the respondent did play a significant role in terms of how respondents viewed education programmes on information management.

The p-value between 'There is low risk of information breaches' and 'Age' is 0.031. This means that there is a significant relationship between the variables, that is, the age of the respondent did play a significant role in terms of how respondents viewed propensity levels of information breaches. The p-value between 'There is low risk of information breaches' and 'Highest level of education completed' is 0.041. This means that there is a significant relationship between the variables, that is, the education level of the respondent did play a significant role in terms of how respondents viewed propensity levels of information breaches. The p-value between 'Information is protected from the moment it is created until the end of its cycle' and 'Staffing level' is 0.006. This means that there is a significant relationship between the variables, that is, the staffing level of the respondent did play a significant role in terms of how respondents viewed the life cycle of information protection.

The p-value between 'I have access to customer information that is not a necessity to perform my job' and 'Staffing level' is 0.000. This means that there is a significant relationship between the variables, that is, the staffing level of the respondent did play a significant role in terms of how respondents viewed their access to customer information. The p-value between 'Money is spent to mitigate data breaches' and 'Staffing level' is 0.013. This means that there is a significant relationship between the variables, that is, the staffing level of the respondent did play a significant role in terms of how

respondents viewed monetary investment to mitigate data breaches. The p-value between 'Money is spent to mitigate data breaches' and 'Area of Specialisation' is 0.015. This means that there is a significant relationship between the variables, that is, the area of specialisation of the respondent did play a significant role in terms of how respondents viewed monetary investment to mitigate data breaches. The p-value between 'Information security is part of my organisational culture' and 'Staffing level' is 0.021. This means that there is a significant relationship between the variables, that is, the staffing level of the respondent did play a significant role in terms of how respondents viewed organisational culture in relation information security. The p-value between 'Information security is part of my organisational culture' and 'How long have you been in this position at the company' is 0.025. This means that there is a significant relationship between the variables, that is, the length of service of the respondent did play a significant role in terms of how respondents viewed organisational culture in relation information security.

The p-value between 'Employees' knowledge is regularly tested on information security policies and procedures' and 'Area of specialisation' is 0.005. This means that there is a significant relationship between the variables, that is, the area of specialisation of the respondent did play a significant role in terms of how respondents viewed testing employees' knowledge on security policies and procedures. The p-value between 'If data breaches do occur there is a set procedures in place that I will follow' and 'Age' is 0.013. This means that there is a significant relationship between the variables, that is, the age of the respondent did play a significant role in terms of how respondents viewed procedures that are followed if data breaches occur.

The p-value between 'If data breaches do occur there is a set procedures in place that I will follow' and 'Staffing level' is 0.029. This means that there is a significant relationship between the variables, that is, the staffing level of the respondent did play a significant role in terms of how respondents viewed procedures that are followed if data breaches occur. The p-value between 'If data breaches do occur there is a set procedures in place that I will follow' and 'How long have you been in this position at the company' is 0.031. This means that there is a significant relationship between the variables, that is, the length of service of the respondent did play a significant role in terms of how respondents viewed procedures that are followed if data breaches occur. The p-value between 'Policies on information management are clear' and 'Age' is 0.044. This means that there is a significant relationship between the variables, that is, the length of service of the respondent did play a significant role in terms of how respondents viewed clarity of information management policies.

The p-value between 'Policies on information management are clear' and 'Staffing level' is 0.011. This means that there is a significant relationship between the variables, that is, the staffing level of the



respondent did play a significant role in terms of how respondents viewed clarity of information management policies. The p-value between 'There are disciplinary measures in place to address employee negligence on information management' and 'How long have you been in this position at the company' is 0.001. This means that there is a significant relationship between the variables, that is, the length of service of the respondent did play a significant role in terms of how respondents viewed how negligence on information management is addressed by disciplinary procedures. The p-value between 'Information security forms part of the annual organisations budgeting' and 'Staffing level' is 0.000. This means that there is a significant relationship between the variables, that is, the staffing level of the respondent did play a significant role in terms of how respondents viewed the organisation's budgeting plans for information security.

The p-value between 'Information security forms part of the annual organisations budgeting' and 'How long have you been in this position at the company' is 0.045. This means that there is a significant relationship between the variables, that is, the length of service of the respondent did play a significant role in terms of how respondents viewed the organisation's budgeting plans for information security. The p-value between 'Technology based solutions are all that is required to ensure information security' and 'Age' is 0.012. This means that there is a significant relationship between the variables, that is, the age of the respondent did play a significant role in terms of how respondents viewed the role of technology based solutions on information security.

The p-value between 'Technology based solutions are all that is required to ensure information security' and 'Staffing level' is 0.036. This means that there is a significant relationship between the variables, that is, the staffing level of the respondent did play a significant role in terms of how respondents viewed the role of technology based solutions on information security. The p-value between 'Without IT systems we cannot control information management' and 'Area of specialisation' is 0.025. This means that there is a significant relationship between the variables, that is, the area of specialisation of the respondent did play a significant role in terms of how respondents viewed the role of IT systems in controlling information management.

The p-value between 'The software systems I use have strict access control to customer information' and 'Age' is 0.004. This means that there is a significant relationship between the variables, that is, the age of the respondent did play a significant role in terms of how respondents viewed the access control of customer information on software systems. The p-value between 'The software systems I use have strict access control to customer information' and 'Area of specialisation' is 0.004. This means that there is a significant relationship between the variables, that is, the area of specialisation of the respondent did play a significant role in terms of how respondents viewed the access control

of customer information on software systems. The p-value between 'The IT systems are aligned with the requirements of protecting customer information' and 'Age' is 0.009. This means that there is a significant relationship between the variables, that is, the age of the respondent did play a significant role in terms of how respondents viewed the functionality of the IT systems for protecting customer information. The p-value between 'The IT systems are aligned with the requirements of protecting customer information' and 'Staffing level' is 0.043. This means that there is a significant relationship between the variables, that is, the staffing level of the respondent did play a significant role in terms of how respondents viewed the functionality of the IT systems for protecting customer information.

The p-value between 'The IT systems are aligned with the requirements of protecting customer information' and 'How long have you been in this position at the company' is 0.035. This means that there is a significant relationship between the variables, that is, the length of service of the respondent did play a significant role in terms of how respondents viewed the functionality of the IT systems for protecting customer information. The p-value between 'Data protection and security protection controls are in place on computers' and 'How long have you been in this position at the company' is 0.040. This means that there is a significant relationship between the variables, that is, the length of service of the respondent did play a significant role in terms of how respondents viewed data and security protection on computers.

The p-value between 'Data protection and security protection controls are in place on computers' and 'Age' is 0.000. This means that there is a significant relationship between the variables, that is, the age of the respondent did play a significant role in terms of how respondents viewed data and security protection on computers. The p-value between 'All interactions with customers are recorded on an IT system' and 'Age' is 0.000. This means that there is a significant relationship between the variables, that is, the age of the respondent did play a significant role in terms of how respondents viewed the recording of customer interactions on IT systems. The p-value between 'All interactions with customers are recorded on an IT system' and 'Staffing level' is 0.018. This means that there is a significant relationship between the variables, that is, the staffing level of the respondent did play a significant role in terms of how respondents viewed the recording of customer interactions on IT systems.

The p-value between 'The IT area is well informed of necessities related to privacy regulation and policies' and 'How long have you been in this position at the company' is 0.001. This means that there is a significant relationship between the variables, that is, the length of service of the respondent did play a significant role in terms of how respondents viewed how informed the IT area is in relation to privacy policies and privacy regulation.

The p-value between 'The standard of information security systems are assessed against international accepted rules and practises' and 'Highest level of education completed' is 0.008. This means that there is a significant relationship between the variables, that is, the education level of the respondent did play a significant role in terms of how respondents viewed how the information security systems are measured. The p-value between 'Employees are required to demonstrate to consumers their level of compliance in relation to information security guidelines' and 'Age' is 0.021. This means that there is a significant relationship between the variables, that is, the age of the respondent did play a significant role in terms of how respondents viewed displaying the level of information security compliance to customers.

The p-value between 'Employees are required to demonstrate to consumers their level of compliance in relation to information security guidelines' and 'Staffing level' is 0.000. This means that there is a significant relationship between the variables, that is, the staffing level of the respondent did play a significant role in terms of how respondents viewed displaying the level of information security compliance to customers. The p-value between 'Employees are required to demonstrate to consumers their level of compliance in relation to information security guidelines' and 'Area of specialisation' is 0.009. This means that there is a significant relationship between the variables, that is, the area of specialisation of the respondent did play a significant role in terms of how respondents viewed displaying the level of information security compliance to customers. The p-value between 'Employees are required to demonstrate to consumers their level of compliance in relation to information security guidelines' and 'How long have you been in this position at the company' is 0.023. This means that there is a significant relationship between the variables, that is, the length of service of the respondent did play a significant role in terms of how respondents viewed displaying the level of information security compliance to customers.

The p-value between 'All business stakeholders are involved when implementing IT systems' and 'Age' is 0.022. This means that there is a significant relationship between the variables, that is, the age of the respondent did play a significant role in terms of how respondents viewed the involvement of different stakeholders when implementing IT systems. The p-value between 'All business stakeholders are involved when implementing IT systems' and 'Area of specialisation' is 0.009. This means that there is a significant relationship between the variables, that is, the area of specialisation of the respondent did play a significant role in terms of how respondents viewed the involvement of different stakeholders when implementing IT systems. The p-value between 'The requirement for risk management is on the decrease' and 'Age' is 0.009. This means that there is a significant relationship between the variables, that is, the age of the respondent did play a significant role in terms of how

respondents viewed the current trend of risk management. The p-value between 'The requirement for risk management is on the decrease' and 'Highest level of education completed' is 0.000. This means that there is a significant relationship between the variables, that is, the level of education of the respondent did play a significant role in terms of how respondents viewed the current trend of risk management.

The p-value between 'The requirement for risk management is on the decrease' and 'Staffing level' is 0.000. This means that there is a significant relationship between the variables, that is, the staffing level of the respondent did play a significant role in terms of how respondents viewed the current trend of risk management. The p-value between 'The requirement for risk management is on the decrease' and 'Area of specialisation' is 0.001. This means that there is a significant relationship between the variables, that is, the area of specialisation of the respondent did play a significant role in terms of how respondents viewed the current trend of risk management. The p-value between 'The requirement for risk management is on the decrease' and 'How long have you been in this position at the company' is 0.016. This means that there is a significant relationship between the variables, that is, the length of service of the respondent did play a significant role in terms of how respondents viewed the current trend of risk management. The p-value between 'Regulatory risks should not form part of the institution's risk plan' and 'Age' is 0.012. This means that there is a significant relationship between the variables, that is, the age of the respondent did play a significant role in terms of how respondents viewed the inclusion of regulatory risks in the organisations risk plan.

The p-value between 'I reactively respond to information risks' and 'Age' is 0.043. This means that there is a significant relationship between the variables, that is, the age of the respondent did play a significant role in terms of how respondents viewed the manner in which they respond to information risks. The p-value between 'I reactively respond to information risks' and 'How long have you been in this position at the company' is 0.025. This means that there is a significant relationship between the variables, that is, the length of service of the respondent did play a significant role in terms of how respondents viewed the manner in which they respond to information risks. The p-value between 'There are instances when I do not get notifications on information risks' and 'Gender' is 0.001. This means that there is a significant relationship between the variables, that is, the gender of the respondent did play a significant role in terms of how respondents viewed whether they receive notifications on information risks. The p-value between 'There are instances when I do not get notifications on information risks' and 'Staffing level' is 0.018. This means that there is a significant relationship between the variables, that is, the staffing level of the respondent did play a significant role in terms of how respondents viewed whether they receive notifications on information risks. The p-value between 'There are instances when I do not get notifications on information risks' and 'Area

of specialisation' is 0.001. This means that there is a significant relationship between the variables, that is, the area of specialisation of the respondent did play a significant role in terms of how respondents viewed whether they receive notifications on information risks. 33 of the 58 statements (Likert scale responses) had one or more statistically significant relationships with the biographical data. 'Age', 'Highest level of education completed', 'Staffing level', 'Area of Specialisation' and 'How long have you been in this position at the company' had a similar amount of significant relationships on the Likert scale responses while 'Gender' had the least amount of significant relationships. The statement 'The requirement for risk management is on the decrease' had the most number of significant relationships.

## 5.6 Correlations

Bivariate correlation was also performed on the (ordinal) data. Positive values indicate a directly proportional relationship between the variables and a negative value indicates an inverse relationship. All significant relationships are indicated by a \* or \*\* (Refer to Appendix D for full results of correlations). Negative values imply an inverse relationship, that is, the variables have an opposite effect on each other. Correlations are discussed below.

The correlation value between "I ensure that I do not breach confidential information" and "Information is protected from the moment it is created until the end of its cycle" is 0.234. This is a directly related proportionality. Respondents indicated that the more that information is protected from creation, the more they would not breach the information, and vice versa. The correlation value between 'I ensure that I do not breach confidential information' and 'I ensure that I secure organisational personal information' is 0.745. This is a directly related proportionality. Respondents indicated that the more they secure organisational personal information, the more they would not breach the information, and vice versa. The correlation value between 'I ensure that I do not breach confidential information' and 'My activities are aligned to government regulations' is 0.234. This is a directly related proportionality. Respondents indicated that the more their activities are aligned to government regulations, the more they would not breach the information, and vice versa. The correlation value between 'My activities are aligned to government regulations' and 'Breaching of information is assessed' is 0.253. This is a directly related proportionality. Respondents indicated that the more information breaches are assessed, the more their belief is that their activities are aligned to government regulations, and vice versa. The correlation value between 'I ensure that I secure organisational personal information' and 'Breaching of information is assessed' is 0.304. This is a directly related proportionality. Respondents indicated that the more information breaches are assessed, the more they ensure that they secure organisational personal information, and vice versa. The correlation value between 'I ensure that I do not breach confidential information' and 'Breaching of information is assessed' is 0.287. This is a

directly related proportionality. Respondents indicated that the more information breaches are assessed, the more they ensure that they do not breach confidential information, and vice versa. The correlation value between 'I ensure that I secure organisational personal information' and 'Employees are trained on information security policies' is 0.233. This is a directly related proportionality. Respondents indicated that the more employees are trained on information security policies, the more they ensure that they secure organisational personal information, and vice versa.

The correlation value between 'Employees are trained on information security policies' and 'Employees keep customer information confidential' is 0.491. This is a directly related proportionality. Respondents indicated that the more employees are trained on information security policies, the more they keep customer information confidential, and vice versa. The correlation value between 'Breaching of information is assessed' and 'Employees keep customer information confidential' is 0.434. This is a directly related proportionality. Respondents indicated that the more breaching of information is assessed, the more they keep customer information confidential, and vice versa.

The correlation value between 'I ensure that I secure organisational personal information' and 'Employees are held accountable for breaching customer data' is 0.288. This is a directly related proportionality. Respondents indicated that the more accountable they are held for breaching data, the more they ensure organisational personal information is secured, and vice versa. The correlation value between 'Employees are trained on information security policies' and 'Employees are held accountable for breaching customer data' is 0.449. This is a directly related proportionality. Respondents indicated that the more employees are trained in information security policies, the more accountable they are held for breaching data, and vice versa. The correlation value between 'Information management security policies are in place' and 'I ensure that I do not breach confidential information' is 0.230. This is a directly related proportionality. Respondents indicated that the more information security policies are put in place, the more they ensure that confidential information is not breached, and vice versa. The correlation value between 'Information management security policies are in place' and 'There are no occurrences of information breaches' is 0.378. This is a directly related proportionality. Respondents indicated that the more information security policies are put in place, the more there would be no occurrences of information breaches, and vice versa.

The correlation value between 'Information management security policies are in place' and 'Employees keep customer information confidential' is 0.446. This is a directly related proportionality. Respondents indicated that the more information security policies are put in place, the more customer information is kept confidential by employees, and vice versa. The correlation value between 'Information management programmes are in place to educate employees' and 'I ensure that I secure

organisational personal information' is 0.227. This is a directly related proportionality. Respondents indicated that the more employees are educated on information management through programmes, the more organisational personal information would be secured, and vice versa.

The correlation value between 'Information management programmes are in place to educate employees' and 'Breaching of information is assessed' is 0.384. This is a directly related proportionality. Respondents indicated that the more employees are educated on information management through programmes, the more information breaching will be assessed, and vice versa. The correlation value between 'Information management programmes are in place to educate employees' and 'Employees are held accountable for breaching customer data' is 0.436. This is a directly related proportionality. Respondents indicated that the more employees are educated on information management through programmes, the more accountable they are held for breaching data, and vice versa. The correlation value between 'Breaching of information is assessed' and 'There is low risk of information breaches' is 0.301. This is a directly related proportionality. Respondents indicated that the more information breaching is assessed, the more there will be a low risk of information breaches, and vice versa.

The correlation value between 'Employees keep customer information confidential' and 'There is low risk of information breaches' is 0.325. This is a directly related proportionality. Respondents indicated that the more customer information is kept confidential, the more there will be a low risk of information breaches, and vice versa. The correlation value between 'Data breaches only occur accidentally' and 'There is low risk of information breaches' is 0.250. This is a directly related proportionality. Respondents indicated that the more data breaches only occur accidentally, the more there will be a low risk of information breaches, and vice versa. The correlation value between 'Employees keep customer information confidential' and 'Information is protected from the moment it is created until the end of its cycle' is 0.492. This is a directly related proportionality. Respondents indicated that the more customer information is kept confidential, the more information is protected from creation, and vice versa. The correlation value between 'Information management programmes are in place to educate employees' and 'Information is protected from the moment it is created until the end of its cycle' is 0.322. This is a directly related proportionality. Respondents indicated that the more employees are educated through information management programmes, the more information is protected from creation, and vice versa. The correlation value between 'I have access to customer information that is not a necessity to perform my job' and 'Employees keep customer information confidential' is -0.242, that is, the more employees keep information secure, the less access one would have to customer information that is not relevant.

The correlation value between 'My activities are aligned to government regulations' and 'I have attended information management training which is beneficial to me' is 0.318. This is a directly related proportionality. Respondents indicated that the more beneficial information management training is, the more their activities would be aligned to government regulations, and vice versa. The correlation value between 'Data breaches only occur accidentally' and 'I have attended information management training which is beneficial to me' is 0.321. This is a directly related proportionality. Respondents indicated that the more beneficial information management training is, the more data breaches would only occur accidentally, and vice versa. The correlation value between 'Information management risks are managed well' and 'My activities are aligned to government regulations' is 0.370. This is a directly related proportionality. Respondents indicated that the more activities are aligned to government regulations, the more information management risks will be well managed, and vice versa.

The correlation value between 'Information management risks are managed well' and 'I have attended information management training which is beneficial to me' is 0.448. This is a directly related proportionality. Respondents indicated that the more beneficial training is received on information management, the more information management risks will be well managed, and vice versa. The correlation value between 'Information management risks are managed well' and 'Information management programmes are in place to educate employees' is 0.487. This is a directly related proportionality. Respondents indicated that the more employees are educated through information management programmes, the more information management risks will be well managed, and vice versa.

The correlation value between 'Information management risks are managed well' and 'Risk assessments are done in order to quantify threats' is 0.449. This is a directly related proportionality. Respondents indicated that the more risks that are done, the more information management risks will be well managed, and vice versa. The correlation value between 'Information is protected from the moment it is created until the end of its cycle' and 'Risk assessments are done in order to quantify threats' is 0.244. This is a directly related proportionality. Respondents indicated that the more risks that are done, the information will be protected from creation, and vice versa. The correlation value between 'Management plays an important role to promote information security' and 'I ensure that I secure organisational personal information' is 0.225. This is a directly related proportionality. Respondents indicated that the more information security is promoted by management, the more organisational personal information will be secured, and vice versa.

The correlation value between 'Management plays an important role to promote information security' and 'Information management risks are managed well' is 0.457. This is a directly related



proportionality. Respondents indicated that the more information security is promoted by management, the more information risks will be managed well, and vice versa. The correlation value between 'Management plays an important role to promote information security' and 'Breaching of information is assessed' is 0.407. This is a directly related proportionality. Respondents indicated that the more information security is promoted by management, the more information breaches is assessed, and vice versa. The correlation value between 'Breaching of information is assessed' and 'Money is spent to mitigate data breaches' is 0.259. This is a directly related proportionality. Respondents indicated that the more money is invested in data breaching mitigation, the more information breaches is assessed, and vice versa. The correlation value between 'Information management security policies are in place' and 'Money is spent to mitigate data breaches' is 0.304. This is a directly related proportionality. Respondents indicated that the more money is invested in data breaching mitigation, the more security policies on information will be in place, and vice versa.

The correlation value between 'I ensure that I do not breach confidential information' and 'Information security is part of my organisational culture' is 0.275. This is a directly related proportionality. Respondents indicated that the more there is a culture of information security, the more confidential information is not breached, and vice versa. The correlation value between 'Employees keep customer information confidential' and 'Information security is part of my organisational culture' is 0.358. This is a directly related proportionality. Respondents indicated that the more there is a culture of information security, the more customer information is kept confidential, and vice versa. The correlation value between 'Information management risks are managed well' and 'Information security is part of my organisational culture' is 0.534. This is a directly related proportionality. Respondents indicated that the more there is a culture of information security, the more information management risks are well managed, and vice versa. The correlation value between 'My activities are aligned to government regulations' and 'There are awareness campaigns on information security' is 0.221. This is a directly related proportionality. Respondents indicate that the more awareness campaigns there are on information security, the more activities are aligned to government regulations, and vice versa. The correlation value between 'Employees keep customer information confidential' and 'There are awareness campaigns on information security' is 0.334. This is a directly related proportionality. Respondents indicated that the more awareness campaigns there are on information security, the more customer information is kept confidential, and vice versa. The correlation value between 'Information security is part of my organisational culture' and 'There are awareness campaigns on information security' is 0.455. This is a directly related proportionality. Respondents indicated that the more awareness campaigns there are on information security, the more information security forms part of the organisational culture, and vice versa. The correlation value between 'Information is protected from the moment it is created until the end of its cycle' and 'Employees' knowledge is

regularly tested on information security policies and procedures' is 0.357. This is a directly related proportionality. Respondents indicated that the more employees knowledge is tested on information security, the more information will be protected from creation, and vice versa.

The correlation value between 'I am aware of government regulations and procedures on information management' and 'Data breaches do not affect its economic condition' is -0.270, that is, the more data breaches do not affect the economic condition, the less aware they are about government regulations and procedures in information management. The correlation value between 'There are awareness campaigns on information security' and 'I am aware of government regulations and procedures on information management' is 0.255. This is a directly related proportionality. Respondents indicated that the more information security awareness campaigns there are, the more awareness there will be of government regulations and procedures on information management, and vice versa.

The correlation value between 'Employees are the strongest link in information security' and 'Information management security policies are in place' is 0.226. This is a directly related proportionality. Respondents indicated that the more policies in place on information management security, the more employees are the strongest link in information security, and vice versa. The correlation value between 'Breaching of information is assessed' and 'If data breaches do occur there is a set procedures in place that I will follow' is 0.407. This is a directly related proportionality. Respondents indicated that the more breaching of information is assessed, the more there is set procedures that will be followed if data breaches occur, and vice versa. The correlation value between 'Employees are trained on information security policies' and 'If data breaches do occur there is a set procedures in place that I will follow' is 0.527. This is a directly related proportionality. Respondents indicated that the more training there is on information security policies, the more there is set procedures that will be followed if data breaches occur, and vice versa. The correlation value between 'Employees keep customer information confidential' and 'If data breaches do occur there is a set procedures in place that I will follow' is 0.527. This is a directly related proportionality. Respondents indicated that the more there is set procedures that will be followed if data breaches occur, the more customer information will be kept confidential, and vice versa. The correlation value between 'Information management programmes are in place to educate employees' and 'If data breaches do occur there is a set procedures in place that I will follow' is 0.465. This is a directly related proportionality. Respondents indicated that the more education there is on information management programmes, the more there is set procedures that will be followed if data breaches occur, and vice versa.

The correlation value between 'Breaching of information is assessed' and 'Information security forms part of the annual organisations budgeting' is 0.298. This is a directly related proportionality. Respondents indicated that the more information security is part of the organisations monetary budget, the more breaching of information is assessed, and vice versa. The correlation value between 'There is low risk of information breaches' and 'Information security forms part of the annual organisations budgeting' is 0.284. This is a directly related proportionality. Respondents indicated that the more information security is part of the organisations monetary budget, the more there will be a lower risk of information breaches, and vice versa. The correlation value between 'Information management risks are managed well' and 'Information security forms part of the annual organisations budgeting' is 0.311. This is a directly related proportionality. Respondents indicated that the more information security is part of the organisations monetary budget, the better information risks are managed, and vice versa.

The correlation value between 'Money is spent to mitigate data breaches' and 'The software systems I use have strict access control to customer information' is 0.321. This is a directly related proportionality. Respondents indicated that the more money is spent to mitigate data breaches, the more access control to customer information will exist on software systems, and vice versa. The correlation value between 'Information is protected from the moment it is created until the end of its cycle' and 'The software systems I use have strict access control to customer information' is 0.439. This is a directly related proportionality. Respondents indicated that the more access control to customer information exist on software systems, the more information will be protected from the point of creation, and vice versa. The correlation value between 'I ensure that I do not breach confidential information' and 'The software systems I use have strict access control to customer information' is 0.303. This is a directly related proportionality. Respondents indicated that the more access control to customer information exist on software systems, the more confidential information will not be breached, and vice versa.

The correlation value between 'Information is protected from the moment it is created until the end of its cycle' and 'The IT systems are aligned with the requirements of protecting customer information' is 0.489. This is a directly related proportionality. Respondents indicated that the more alignment there is between IT systems and protecting customer information, the more information will be protected from the point of creation, and vice versa. The correlation value between 'Employees keep customer information confidential' and 'Data protection and security protection controls are in place on computers' is 0.329. This is a directly related proportionality. Respondents indicated that the more data and security protection there are on computers, the more customer information is kept confidential, and vice versa.

The correlation value between 'Data breaches only occur accidentally' and 'Employees have access to pass customer information to a third party e.g. via email' is -0.223, that is, the more customer information can be transferred, the less data breaches will only occur accidentally. The correlation value between 'Employees are held accountable for breaching customer data' and 'All interactions with customers are recorded on an IT system' is 0.363. This is a directly related proportionality. Respondents indicated that the more IT systems record customer interactions, the more accountability is placed on employees for breaching customer data, and vice versa. The correlation value between 'There is low risk of information breaches' and 'All interactions with customers are recorded on an IT system' is 0.242. This is a directly related proportionality. Respondents indicated that the more IT systems record customer interactions, the more there is a low risk of information breaches, and vice versa. The correlation value between 'The IT systems are aligned with the requirements of protecting customer information' and 'All interactions with customers are recorded on an IT system' is 0.482. This is a directly related proportionality. Respondents indicated that the more IT systems record customer interactions, the more aligned IT systems are to protect customer information, and vice versa.

The correlation value between 'Information is protected from the moment it is created until the end of its cycle' and 'The IT area is well informed of necessities related to privacy regulation and policies' is 0.403. This is a directly related proportionality. Respondents indicated that the better the IT are informed of privacy regulation policies, the more information is protected from its creation, and vice versa. The correlation value between 'The software systems I use have strict access control to customer information' and 'The standard of information security systems are assessed against international accepted rules and practises' is 0.392. This is a directly related proportionality. Respondents indicated that the more the information security systems are benchmarked against international standards, the more software systems used will have strict access control to customer information, and vice versa. The correlation value between 'The software systems I use have strict access control to customer information' and 'The IT area is well informed of necessities related to privacy regulation and policies' is 0.683. This is a directly related proportionality. Respondents indicated that the more the information security systems are benchmarked against international standards, the more the IT department will be informed on privacy regulation and policies, and vice versa.

The correlation value between 'Employees are required to demonstrate to consumers their level of compliance in relation to information security guidelines' and 'There are disciplinary measures in place to address employee negligence on information management' is 0.500. This is a directly related

proportionality. Respondents indicated that the more disciplinary measures in place to address negligence on information management, the more information security compliance levels are required to be demonstrated to consumers, and vice versa. The correlation value between 'The IT area is well informed of necessities related to privacy regulation and policies' and 'All business stakeholders are involved when implementing IT systems' is 0.480. This is a directly related proportionality. Respondents indicated that the more involved all business stakeholder are when implementing IT systems, the more informed the IT department is on privacy regulation and policies, and vice versa.

The correlation value between 'Management plays an important role to promote information security' and 'The requirement for risk management is on the decrease' is -0.235, that is, the more risk management does not form part of business requirements, the less information security is promoted by management. The correlation value between 'Breaching of information is assessed' and 'Regulatory risks should not form part of the institution's risk plan' is -0.267, that is, the more regulatory risks does not form part of the organisations risk plan, the less information breaching is assessed. The correlation value between 'Information management security policies are in place' and 'There are no contingency plans in place to deal with risks on information management' is -0.431. That is, the more contingency plans on information management are absent, the less policies on information security exist.

The correlation value between 'Employees keep customer information confidential' and 'Information is not securely backed up in the event it should be lost' is -0.343, that is, the more information is not backed up and lost, the less customer information is kept confidential by employees. The correlation value between 'I am not able to identify information risks' and 'My activities are aligned to government regulations' is -0.233, that is, the more information risks are not identifiable, the less government regulations are aligned with my working activities. The correlation value between 'There are no controls in place to react to information management risks' and 'I reactively respond to information risks' is 0.221. This is a directly related proportionality. Respondents indicate that the more no controls are available to react to information management risks, the more reactively they respond to information risks, and vice versa. The correlation value between 'We do not respond well to risks on information management' and 'There are instances when I do not get notifications on information risks' is 0.390. This is a directly related proportionality. Respondents indicated that the more no notifications are received on information risks, the worse they respond to risks on information management, and vice versa.

## **5.7 Summary**

This chapter illustrated and explained the data analysis and statistics obtained from the research study questionnaire. The findings and observations from the statistics and data analysis in this chapter are further explained in more detail in Chapter 7 of this research study.

The next chapter, Chapter 6, presents the second data presentation and analysis chapter whereby the information gathered from the semi structured in-depth interviews are analysed.

## **CHAPTER SIX: DATA PRESENTATION AND ANALYSIS (b)**

### **6.1 Introduction**

This chapter presents the trends and patterns while discussing the findings obtained from the semi-structured in-depth interviews in this study. The data collected from the research study's semi structured in-depth interviews was analysed whereby patterns were identified and trends categorised into themes in line with the research study's main objective. The interviews were conducted with senior management in the organisation. These senior managers are responsible for different areas of the value chain within the organisation in study.

### **6.2 In-depth interview findings**

In addition to the biographical questions highlighted in Chapter 4, the questions in the interviews covered a further 5 dimensions. The questions were based on the dimensions of breaching of data in a financial institution, information management mitigation in a financial institution, information management preparedness in a financial institution, information management systems in a financial institution and risk response and recovery in a financial institution.

#### **6.2.1 What plans do have to ensure that employees do not breach information in this organisation?**

The majority of respondents indicated that there are policies in place on breach notification at the organisation, even if those policies are not standard across the organisation. There are 6 respondents who highlighted the IT security policy and security architecture is in place whereby external devices such as USB's and other portable devices are blocked by the company computers. Employees can, therefore, not transfer information from company computers onto their own personal devices. Password protected computers, as part of the broader IT security policy, also came through from respondents while other respondents added that system changes related to data privacy and data security are done by the Enterprise Project Office (EPO) department.

There are 2 respondents who made mention of company policy which informs employees about data breaches. There are breaching of confidentiality awareness exercises done, as noted by 1 respondent. It was highlighted by 1 respondent that certain policies are rolled out through data stewards who form part of the Data Governance Council (DGC). There is 1 respondent who stated that there is no visibility of controls, and there are 2 respondents who spoke of a policy of not having mobile phones and smart phones in operational areas. It was noted by a respondent that investigations are done on data breaches while other respondents added that disciplinary actions are taken against employees who breach information. Furthermore, 1 respondent added to the

technological aspect of data breaches at the organisation stating that penetration tests and vulnerability assessments are done on the technology used.

Another theme that came through strongly in relation to data breaching is email security. There are 4 respondents who highlighted there that is email control at the organisation whereby emails are monitored through technology to detect if users are sending an email with sensitive information in it, such as South African ID numbers. These emails send a trigger to alert the operational risk area as well as the line manager of the user who wants to send the email. There are also trigger alerts sent when documents with sensitive information are printed. There are 2 respondents who further noted that the FTP (File Transfer Protocol) and SFTP (Secure File Transfer Protocol) are used when their staff need to send sensitive information to external vendors.

Certain 'house rules' such as having a clean desk policy was noted by 2 respondents. The clean desk policy aims at ensuring that no customer information is left on work desks of employees. In addition, 1 respondent added that team leaders are requested to check that there are no papers left on desks after every shift is completed. The respondent made note of external cleaning staff that come into the building at night who would also, therefore, have access to customer information if left on desks. This would, therefore, constitute data breach. It is mentioned that there is a plan for breaches, but it could be better. One senior management member exemplified this by stating: *"We are going to be putting in new systems, policies, procedures, monitoring around understanding across the board, both users and the back end into servers, what they using, when they using it, how they using it and trying to also come up with system breaches. The reality of the fact is that we are not there, we have a long way to go but we started the process to mature ourselves in that context."*

### **6.2.2 Do you have policies in this institution dealing with information management? Yes/No.**

There are 8 out of the 9 respondents who answered yes to the question while 1 respondent answered no stating that there are no policies in place in their department specifically on information management and that they only have a user control document that is access-controlled whereby no one else in the organisation can access this document. Another respondent who answered yes added that the DGC ensures policies and procedures are there, but there are still gaps.

### **6.2.3 If yes, are they responsive or aligned to national legislations?**

There are 3 respondents who mentioned the Protection of Personal Information Act (POPI) and that even though it is not yet in place, POPI is the closest legislation dealing with information management. There is 1 respondent who also mentioned the Consumer Protection Act (CPA) as legislation that the



organisation and its policies are aligned to, the human resources protocol for data breaches in the organisation while another respondent added that the organisation has Non-Disclosure Agreements (NDA) in place with vendors to protect its information. It was also noted that there are a lot of non-legislative controls and monitoring in place. There are 2 respondents who added that the way information is passed from one person to another is checked. This speaks to the non-legislative controls and monitoring in place. Another respondent added that it is a work in progress to get everything and everyone aligned. POPI was a strong theme that came through under legislation. It is, however, mentioned that the organisation is still coming to grips with the requirements of POPI. One senior management member brought this across by stating that: *“We obviously have a POPI project running and it’s on our radar so we trying to take the appropriate steps so that when it does become available we will manage our data in a responsible fashion as a responsible party for data.”*

#### **6.2.4 What are the opportunities and challenges brought by this policy?**

The majority of respondents commented on the challenges brought about by policies while only 2 respondents highlighted both challenges as well as opportunities. The policies that respondents noted brought about challenges are POPI and the National Credit Act Amendment (NCAA). The types of challenges resulting from these policies that came through strongly were data capturing by assessing the way data is obtained, what is done with data once it is obtained, the fact that data can only be kept for specific purposes and that sharing data can also now become a challenge as there are different elements of data privacy. There is 1 respondent who added that there is a lot of legislation on the finance industry in South Africa to an extent that it can be said that the South African financial sector is over-governed. The theme of losing out on opportunity and costs and efficiency came through as 3 respondents noted that it takes time to implement the operational process stemming from the policies into the current customer acquisition process. It is stated that there are usually additional processes required, the policy could cause more monetary costs to the organisation and that implementing new processes because of policy eats into the time that could have been spent on implementing new strategies to increase revenue. There are 2 respondents who added that it is labour-intensive to implement policies and that it reduces flexibility and creativity.

There are 2 respondents who highlighted technology constraints when implementing policies while another respondent leaned more towards the people aspect by stating that a big challenge is keeping policies in mind for staff and ensuring that staff members abide by the policies. The 2 respondents who highlighted opportunities brought about by policies stated that policies ensure that there is a clear standard and guideline, compliance is defined and that policies reinforce privacy by giving staff and customers the assurance that information is safe. The opportunities are epitomised by one senior

manager stating that: *“the opportunity is that there is a clear guideline and standard that everybody is aware of and complies with.”*

#### **6.2.5 What organisational plans are in place to ensure that your key stakeholders (employees, vendors, etc.) do not breach information?**

There were 3 themes that came through under this question. A) Contracts with vendors; B) employee policy and education; and C) IT security. There are 2 respondents who noted that there are contracts in place with external vendors who have access to any information belonging to the organisation and that there are clauses in the various contracts stating what can be done with the data or information. There are 4 respondents who highlighted that there are policies in place for employees and that educating employees is an important aspect of breaching information. There are 2 respondents who added that there are email alerts on breaches and that external devices are blocked, which also came through in section 6.2.1.

#### **6.2.6 What tools do you have in place to ensure that your key stakeholders do not breach information?**

There were similar themes found in this as section as there were in section 6.2.5. The tools used were elaborated on more by respondents as 5 respondents made mention of IT security used by the organisation. These included email alerts and email blocking, blocking portable devices, password protection on computers, web sense on certain online sites and having FTP sites available. There are 2 respondents who highlighted employee involvement through house rules and policies and online modules to educate employees.

#### **6.2.7 Do you have, in this organisation, mitigation strategies on information management? Yes/No.**

There are 7 out of the 9 respondents who answered yes while the balance of 2 respondents answered *no* to the question.

#### **6.2.8 What are your mitigation plans in relation to information management?**

There was theme of controls, policies and process highlighted by 3 respondents. Coming from this theme, respondents made mention of controls and policies put in place by the organisation to mitigate the negative risks relating to information management. It was noted that there are business continuity planning and business risk processes as well as a human resource disciplinary processes at the organisation. In addition, there is data governance which is led by the DGC and filters through to the data stewards via a memorandum of understanding. The DGC has regular meetings to discuss data and information management. One senior management member exemplified the fact of using policies

and processes as a mitigation plan by stating that: *“if there is a control missing or maybe there’s a problem in a system to deal with it and maybe it’s something we not dealing with in the policies we can put that in place.”*

There are 7 respondents who made reference to technology being used as a form of mitigation. Of these respondents, 4 highlighted the fact of alerts, password protection, blocking external devices and data restrictions, as discussed previously. In addition, respondents made reference to firewall technology, virus management technology and a master data management tool. Moreover, 1 of the 7 respondents added that the technology could be improved while another noted that: any user can take screenshots on computers, laptops are not encrypted and was opposed to previous respondents’ perceptions of email control by stating that emails are uncontrolled. Another theme that was found is that of the consistency of information and information governance. There is 1 respondent who noted that there is now a central governance function in the DGC to deal with information while another respondent added through the DGC all matters dealing with information management will filter through to business silos so that everyone is aware.

There is 1 respondent who was in disagreement to this by stating that there is no consistent view of information and that data is sporadic around in the organisation. Furthermore, it is mentioned that this causes a challenge for business intelligence to take place. Following the theme and discussion of inconsistency, 3 respondents made reference to a strategy and roadmap to manage data and information. This is emphasised by one senior manager in saying that: *“We take for granted that data is also good for what we do as a business but it can also be to our demise if something goes wrong so I think overall strategy is that we finally have an owner for data governance.”*

**6.2.9 Are all staff members, other than executive management, aware and knowledgeable of the information management security policies put in place by the organisation?  
Yes/No.**

There were 7 of the 9 respondents who answered *yes* to the question, 1 respondent answered *no* and 1 respondent stated *“I don’t think they are as aware as they could be”*.

**6.2.10 If yes, what is done in order to achieve this? If no, what does the organisation view as being important in relation to information management?**

There are 5 respondents who made mention of awareness campaigns to inform employees. There are 3 of the 5 respondents who mentioned that online learning modules available on the intranet are used to inform staff. There is 1 respondent who highlighted that the organisation is trying to increase the awareness while another respondent added that the organisation is always trying to get

awareness to a higher level. Another theme that came through once more was policies that are in place. There is 1 respondent who mentioned that there are employment contracts in place with specified policies and procedures while another respondent added that there are social media policies, IT system acceptable user policies and that all employees must abide by these. It is noted that staff have to acknowledge regulations when logging onto computers by accepting terms and conditions. One senior member management member brought this across by stating that: *"policies will be listed on this log shortly, with a clear expectation that you know what these polices mean and you have to abide by them. If you don't know what they are get hold of your manager to figure it out because ignorance is not going to be an excuse to the regulator"*. There is 1 respondent who answered *no* to the question, stating that the organisation lacks execution and needs to be more conscious and cautious on issues relating to information management.

#### **6.2.11 Do you have preparedness plans to respond to any potential risk on information management? Yes/No.**

There are 6 respondents who answered *yes* while 3 respondents answered *no*. Of the respondents who answered *yes*, 2 respondents made reference to the disciplinary process and industrial relations process whereby employees could be suspended while another added that the organisation has a breach management and crisis management policy. The theme of policy comes through once more with focus on human resource policies and disciplinary and operation risk policy in the form of breaches and crisis management. There is 1 respondent who answered *no*, stating that preparedness plans are on the organisation's to-do list while another respondent was opposed to this by answering that there are analyses done to make sure preparedness plans are in place. It is further mentioned that the analysis is done by the Information Technology Risk Committee at the organisation. This is exemplified by one senior management member stating that: *"It will be logged there and it will be driven through whoever the stakeholder is that's involved. They need to come up with a plan they need to come up with ownership, they will deal with it that way. So plan and process, yes."*

#### **6.2.12 How are government policies and regulations on information management aligned with this organisation's policies?**

There are 4 respondents who highlighted specific policies that the organisation is aligned to as well as legislation that the organisation is preparing for. It is noted that the organisation is aligned to the CPA, Direct Marketing Association (DMA) while POPI is being prepared for. There is 1 respondent who stated that internal and external audits are done to close any gaps while another added that audits are based on legislation and group governance. One respondent noted that there is no specific requirement on confidentiality and that it is more about a code of ethics while another respondent highlighted that controls and execution are lacking at the organisation by stating that *"we take it*

*seriously but we lacking in the execution and control of it*'. 1 respondent however stated that the policies are planned through projects and is done at executive level.

### **6.2.13 How are the organisation's technology systems aligned to the strategic plans of the organisation in relation to information management?**

There are 5 respondents who commented on how systems are used positively in the organisation. There are 2 respondents who made mention of users' rights whereby different users have different access rights to systems and systems that govern access to information. Another respondent noted that systems are password-protected and that only 3 people in the organisation have access to the payroll system. There is 1 respondent who added that information cannot be sent directly off any of the systems in their area while another added that there is a project in place to have one system control access to information. There is 1 respondent who further spoke about this project being a master data management project. There are 2 respondents who were in disagreement by stating that the current systems are not aligned and that the organisation has a long way to be fully compliant while there is high risk of error. One senior management member exemplified this by stating that: *"It can't be done in our current systems from an information management perspective, well it can be done but then it's done manually and ineffectively, it's not optimal and there's a high risk of error. For the future target architecture, we are busy putting together what it will look like and this will have to address these things"*.

### **6.2.14 If it's not aligned, why?**

The concept of the organisation lacking execution came through once more.

### **6.2.15 What are the organisation's risk management plans to deal with information management breaches?**

It was noted that risk management is mainly looked after by the operational risk manager. There are 2 respondents who highlighted that forensic training and forensic audits are done to investigate data breaches. One senior management member stated that: *"We've done some forensic training to make sure that if we ever have a breach that we are able to secure the data we would need for the forensic investigation"*. The involvement of the operational risk area,, therefore filters through 4 respondents, which creates the operational risk management theme. There are 3 respondents who noted that alerts and early warning signals are in place. Further technological plans that were added by respondents are voice recordings and backup strategies on voice recordings that are in place at the organisation as well as employees capturing customer information online as opposed to writing it down on paper. It is added by 1 respondent that where employees writing down information on paper, there are 'clear

data' safety bins whereby all papers can be safely disposed. There is 1 respondent who noted that risk management plans at the organisation are reactive.

### **6.3 Summary**

This chapter highlighted themes and patterns and explained the data analysis obtained from the research study's semi structured in-depth interviews. The findings and observations from the themes and data analysis in this chapter are further explained in more detail in the next chapter of this research study, which is Chapter 7.

In Chapter 7, the literature sources reviewed in Chapters 2 and 3, the research study's main investigative questions and objectives from Chapter 4 are all revisited to ensure the application of the research methodologies and literature consulted correlates to the findings and observations extracted by the researcher and statistician from the data analysis chapters.

## CHAPTER SEVEN: DISCUSSION OF FINDINGS

### 7.1 Introduction

This chapter discusses the data findings from the qualitative and quantitative data collected and analysis done on the data the findings. The literature reviewed in Chapters 2 and 3 are compared to the findings while the major highlights of this study are discussed in alignment with the investigative questions and objectives of this study.

### 7.2 Breaching of data in a financial institution

Just under ½ of the respondents did not disagree to the statement in the questionnaire that at their financial institution, customers are not concerned about information management. In addition, 1/3 of respondents did not disagree to the statement in the questionnaire that data breaches have a positive impact. These are, therefore, in disagreement with Malhotra and Malhotra (2011:46) who note that when customer information is breached by organisations, it has a long-term negative impact on the organisation. This is also in disagreement with Bulgurcu, Cavusoglu and Benbasat (2010: 524) who explain that the risk of information security breaches could result in a loss of creditability for the organisation as well as monetary damage. Zhang, Reithel and Li (2009: 330-338) add that information security breaches can affect an organisation's reputation by damaging customer confidence in the organisation, which is in disagreement with a fair amount of respondents who did not disagree with the two statements in question. There are 39% of respondents who did not disagree to the statement in the questionnaire that data breaches do not affect the economic condition of the organisation (33% undecided and 6% disagree). This is in disagreement with Zhang, Reithel, and Li (2009: 330-338) who state that data and security breaches negatively impacts the economic condition of the organisation.

There are 34% of respondents who did not agree to the statement in the questionnaire that breaching of information is assessed. This is in disagreement with Abu-Musa (2012: 236) who states that one of the key factors to a comprehensive information security programme is a periodic assessment of risks and business impact analyses. Chen, Pedrycz, Ma and Wang (2014: 687) state that information security risk assessment can quantify risk management through the analysis, which is, therefore, also in disagreement. There are 69% of respondents who disagreed to the statement in the questionnaire that data breaches only occur accidentally. The majority of respondents are in agreement with D'Arcy and Green (2014: 474) who highlight that employees may, at times, violate information policies and guidelines with the purpose of harmful intentions such as stealing organisational information or sabotaging the organisation

The minority of respondents (10% disagree) were, however, in agreement with Frangopoulos, Eloff and Venter (2013: 54) who note that breaches could occur deliberately or accidentally as a result of employee negligence.

There are 26% of respondents who did not agree to the statement in the questionnaire that employees are trained on information security policies. This is in disagreement with Abu-Musa (2012: 236) who notes that training in the operation of security process is key to information security while Fourie (2011: 387-389) states that information professionals need to provide training and support as part of the promotion process of personal information management. Hagen and Albrechtsen (2009: 388-405) add that training and educating employees is more effective than formal procedures and controls put in place by the organisation, but many organisations do not provide adequate training to employees in relation to information security.

There are 28% of respondents who did not agree to the statement in the questionnaire that employees keep customer information confidential. These respondents are in agreement with Thompson and Van Niekerk (2012: 39-43) who note that employees can often be the weakest link when it comes to safeguarding information security. This is likely due to an unconcern of information security as individual employees may not feel that it is their responsibility to protect this information. In addition to employees not keeping information safe, findings from the in-depth interviews highlighted that there are policies on information management at the organisation; however, these policies are not standard across the organisation. This supports the fact that in the questionnaire responses, 28% of respondents did not agree to the statement in the questionnaire that employees keep customer information confidential. Furthermore, under the dimension of breaching data in a financial institution, the in-depth interviews made reference to external cleaning staff coming in during the evening and would have access to customer information if it is left on desks. This would constitute data breach. This cause of a data breach is not mentioned in previous literature reviewed.

### **7.3 Information management mitigation in a financial institution**

There are 31% of respondents who agreed to the statement in the questionnaire that there is a low risk of information breaches; therefore, majority of respondents were undecided and disagreed. This is in disagreement with Smith, Dinev and Heng (2011: 990) who state that there is a growing increase in concern for information privacy by governments, business and consumers. There are 38% of respondents who agreed to the statement in the questionnaire that information is protected from the moment it is created until the end of its cycle; therefore, the majority did not agree (35% undecided and 27% disagree). This is in disagreement with Gable (2014: 39) who notes that an Information Governance (IG) programme should be adopted to protect private information which ensures that personal information is protected from the moment it is created to the time it undergoes final



disposition. In addition, from the findings in the in-depth interviews, it is revealed that there is a data governance council that has been formed at the organisation, but it is also noted by respondents in the qualitative results that there are new procedures being put in place but that there is still a long way to go for the organisation to excel in this context. The fact that there is still a substantial amount of work to be done supports the majority of respondents not agreeing to the statement on information protection in the questionnaire.

The responses show that ½ of respondents disagreed to the statement in the questionnaire: 'I have attended information management training which is beneficial to me'. This is in disagreement with Zhang, Reithel and Li (2009: 330) who state that trained employees are important security counter-measures to breaching information in an organisation while Hagen and Albrechtsen (2009: 388-405) add that training and educating employees is more effective than formal procedures. Furthermore, in the qualitative results, the concept of policies and awareness programmes came through by respondents but not training on information management. This supports the results from the quantitative study where respondents stated that they have not received training on policies.

There are 48% of respondents who did not agree to the statement in the questionnaire that information management risks are managed well (38% undecided and 10% disagree). There is, therefore, a mixed perception of how information management risk is managed at the organisation. According to Nazimoglu and Ozsen (2010: 351), before risks can be managed, the risks need to be identified. Risk management is a structured approach which manages uncertainty through risk assessments, strategies and risk mitigations and handles the effects of risks and reduces the negative effects of these risks. This, therefore, highlights that risk identification are not at the forefront at the organisation and that risk assessments may be lacking. The qualitative results proved that controls and policies are put in place by the organisation to mitigate the negative risks relating to information management. It was noted that there are business continuity planning and business risk processes as well as human resource disciplinary processes at the organisation. However, the concept that policies may not be the most effective form training and education for employees speaks to the mixed perceptions of respondents to the statement in the questionnaire. These mixed perceptions are further represented by 52% of respondents agreeing to the statement in the questionnaire that 'risk assessments are done in order to quantify threats' (42% undecided and 6% disagree). Chen, Pedrycz, Ma and Wang (2014: 687) are in agreement with the difficulty of risk assessments as represented by the dissimilar responses in this study's results to information risk by stating that 'information risk assessment is a complex process which at times is a real-time process'.

There are 67% of respondents who agreed to the statement in the questionnaire that 'information security is part of my organisational culture' while 63% of respondents agreed to the statement in the questionnaire that 'there are awareness campaigns in information security at the organisation'. The approximately 1/3 of respondents who were in disagreement are supported by the qualitative results that policies and procedures are not standard across the organisation and that there are still business silos. The disagreements are in line with Lacey (2010: 7) who notes that organisations have not yet defined precisely what security culture actually entails.

The majority of agreements to the statements in the quantitative results are in agreement with Van Niekerk and Van Solms (2010: 477) who state that there should be an information security culture adopted by organisations in order to obtain the required information security and that organisations need to adopt a culture whereby information security forms part of the organisational culture to influence employees' behaviour towards information security. The majority of results from the questionnaire are further supported by the qualitative results whereby respondents made mention of awareness campaigns on information management and online learning modules to inform staff of information management related activities. In addition, 37% of respondents both agreed and disagreed that employees' knowledge is regularly tested on information policies and procedures while 26% were undecided.

In addition to non-standardised processes across the organisation, as discussed previously Bulgurcu et al. (2010: 524) mention that employees can, at times, be the weak link in information security while Thompson and Van Niekerk (2012: 39-43) add that employees can often be the weakest link when it comes to safeguarding information security. Desai and Von de Embse (2008: 20-26) note that there is a great deal of focus on employee practices as this could have legal concerns associated to it. The qualitative results do highlight policies and procedures on numerous occasions; however, employee-testing of these policies and procedures was not mentioned. The qualitative result on this, therefore, supports the quantitative result.

#### **7.4 Information management preparedness in a financial institution**

There are 78% of respondents who agreed to the statement in the questionnaire that employees are the strongest link in information security. This majority of respondents are in disagreement with Bulgurcu, Cavusoglu and Benbasat (2010: 524) and Thompson and Van Niekerk (2012: 39) who state that employees could be seen as the weak link in information security. Approximately 1/3 respondents did not agree to the statement in the questionnaire that 'if data breaches do occur, there is set procedures in place that I will follow'. This is in disagreement with Abu-Musa (2012: 236) who advises that having a framework of practises and procedures are important factors in information security.

From the qualitative results, 1/3 respondents noted that there are no information management preparedness plans at the organisation. The percentage and perceptions of the qualitative results are, therefore, in line with that of the quantitative results. More than 1/3 respondents did not agree to the statement in the questionnaire that policies on information management are clear. The majority of respondents from the qualitative results regularly noted that there are policies in place at the organisation to deal with information. There is, therefore, misalignment whereby there are policies, but it may not be clear to all staff. Knapp, Morris, Marshall and Byrd (2009: 2) explain that a policy is a general rule passed by the organisation to limit the discretion of employees while Garrison and Ncube (2011: 216-217) add that it is of importance that organisational policies are in place to quickly respond to data breaches. In addition, it is also added by D'Arcy and Green (2014: 474) that to encourage employees to comply with authorised information security policies is a great challenge for organisations.

There are 77% of respondents who agreed to the statement in the questionnaire that there are disciplinary measures in place to address employee negligence on information management. This is supported by the qualitative results whereby it is stated that disciplinary action is taken against employees who breach information. This is in agreement with Abu-Musa (2012: 236) that there should be employee accountability in relation to information security. There are 38% of respondents who agreed to the statement in the questionnaire that information security forms part of the annual organisations' budget while 53% were undecided and 9% disagreed. The majority of respondents were in disagreement with Stewart (2012: 312) who highlights that certain organisations who take information security into account when doing their financial budgeting increase the effectiveness of the spending for the organisation, stakeholders and customers.

## **7.5 Information management systems in a financial institution**

There are 64% of respondents who disagreed to the statement in the questionnaire that technology based solutions are all that is required to ensure information security. These respondents are in agreement with Herath and Rao (2009: 154) who state that information systems is a crucial area for organisations in order to protect information, but technology is not sufficient as end-user security behaviour is gaining more attention and can also prove more difficult to monitor. There are, however, still 36% of respondents (22% undecided and 14% agree) who do not agree with Herath and Rao (2009). In the qualitative results, both technological and non-technological systems, such as policies, were identified by respondents as solutions to information security adopted by the organisation. The majority of respondents (74%) agreed to the statement in the questionnaire that 'without IT systems, we cannot control information management'. Katos and Patel (2008: 78) note that the demand for privacy security technology depends on the level of security required whereby the higher the level of

privacy information needed, the more security systems may be demanded; Nazimoglu and Ozsen (2010: 351) add that technology has become the backbone of commerce. The respondents to the qualitative analysis highlighted technological systems used to protect information such as email alerts, passwords on computers, firewall technology, virus management technology and a master data management tool.

Moreover, 86% of respondents agreed to the statement in the questionnaire that data protection and security protection controls are in place on computers. This is in agreement with D'Arcy and Green (2014: 476) who note that computer monitoring is an important concept of security culture in organisations. This is supported by the qualitative results whereby respondents highlighted that external devices such as USBs and other portable devices are blocked by the company computers. Employees cannot transfer information from company computers. This is further supported by respondents to the in-depth interviews stating that there is password protection on computers. Moreover, 63% of respondents agreed to the statement in the questionnaire that employees have access to pass customer information to a third party e.g. via email. Although it was stated by respondents in the qualitative results on numerous occasions that there are email alerts and email blocking on sensitive information, 1 respondent noted that emails are uncontrolled while another stated that the organisation has a long way to be fully compliant and that there is high risk of error.

There is therefore misalignment between senior management's perceptions and that of non-senior management employees. Gal and Berente (2008: 133-150) state that implementing information systems is a complex process whereby all stakeholder groups have to be involved as their needs and requirements are different, and their understanding or perception of the technology may be different. People's interpretation of the purpose of the technology may vary, so it is of importance to involve all stakeholders. These interpretations could have a substantial impact on the success of the implementation of the information systems. The implementation of information systems cannot only be looked at from a technological perspective or framework as social representations also have to be addressed. Social representations could give a more fundamental approach to information system implementation. This social representations theory includes shaping the organisational members' perceptions to the technology, thereby affecting the success of the implementation of these technologies.

There are 49% of respondents who agreed while 48% were undecided to the statement in the questionnaire that 'the standards of information security systems are assessed against international accepted rules and practises'. There is a big divide in perception and awareness in this regard. According to Tsohou, Kokolakis, Lambrinouidakis and Gritzalis (2010: 351), there should be

standardisation of information security systems as this will provide conformity assessment mechanisms to ensure that it meets international accepted rules and practises. From the qualitative results it was noted that there is a project in place to have one system control access to information. There are 41% of respondents who were undecided to the statement in the questionnaire that all business stakeholders are involved when implementing IT systems, 36% agreed and 23% disagreed. As highlighted previously, Gal and Berente (2008: 133) state that all stakeholder groups have to be involved when implementing information systems as their needs and requirements are different. There are, therefore, mixed perceptions and views to this statement by respondents whereby most of respondents do not agree that they are involved in implementing IT systems. There are 43% of respondents who were in agreement to the statement in the questionnaire that information systems are becoming more exposed to risk and breaches; 40% were undecided while 17% disagreed. Al-Mukahal and Alshare (2015: 102-103) note that there is a rising number in security risk incidents and that information systems are becoming more exposed to risk and breaches. A large percentage of respondents (57%), therefore, did not agree with the statement by Al-Mukahal and Alshare (2015).

## **7.6 Risk response and recovery in a financial institution**

The responses to the statement in the questionnaire that 'I reactively respond information risks' had almost an equal mix across selection categories (37% agree, 33% disagree, 30% undecided). In the qualitative results, 1 respondent noted that risk management plans at the organisation are reactive. The inconsistency in responses from the questionnaire highlights previous findings of the variation that may exists across departments within the organisation. Caldwell (2008: 163-166) states that when proactive rather than reactive decisions are made, the return on value from information is maximised. There are 39% of respondents who agreed to the statement in the questionnaire that 'there are instances when I do not get notifications on information risks'. There are 35% who disagreed and 26% were undecided. The results from the qualitative results indicated that line and managers and the operational risk area gets notifications on information risks. According to Pike (2009: 16-17), in the United States, there are over 40 states that passed legislation which requires organisations to provide notification of data breaches.

## **7.7 Summary**

This chapter highlighted the major findings obtained from the quantitative and qualitative analysis. Major findings include, but are not limited to, lack of training on information management policies, external cleaning staff potentially having access to organisational customer information and the lack of budgeting for information security at the organisation. Some findings such as the lack of training

was discovered across different dimensions of this study. The next chapter provides recommendations for the organisation based on the major highlights from this chapter.

## **CHAPTER EIGHT: CONCLUSION AND RESOMENDATIONS**

### **8.1 Introduction**

This study has been guided by investigating the shortfalls of information security in a selected South African financial institution, investigating contingency plans (preparedness, mitigation, response and recovery) effective for any forthcoming risk, and changes the organisation need to consider adopting as a result of information security. This chapter is split into 3 sub-sections namely: recommendations for the organisation, guidelines for future researchers and limitations to the study. In this chapter, conclusions and recommendations are drawn from the discussed findings in Chapter 7.

### **8.2 Conclusion**

The objectives of this study were to explore: the shortfalls of information security on a South African financial institution; data privacy; responsiveness of business processes and capability of systems on information management. The study further investigated strategies formulated and projects and programmes for information management; contingency plans on how to respond to the financial risk in respect to information management and provide recommendations based on the empirical findings. This study explored and investigated all of these objectives through a mix of both qualitative and quantitative research and by splitting the study into different dimensions. This study reached several conclusions based on the empirical findings. Firstly, the results of the analysis concludes that there are big deficiencies for training officers to conduct beneficial information management training at the organisation. This training covers a number of different aspects of information management. This implies that all areas of the organisation were under-skilled on various characteristics or aspects of information management which could have detrimental consequences for potential data breaches.

Secondly, an information security programme that includes business risk analysis is not implemented in this financial institution. This implies that there are not proper investigations and pre-work done by the organisation to base future information management strategies on. Thirdly, a standardised or uniform house rule policy is not consistently implemented across the organisation. This implies that each department or team within departments can decide not to apply any house rules, which could lead to data breaches. Fourthly, the external cleaning company is not signing a Non-Disclosure Agreement with the organisation. This implies that if external cleaning staff should find customer information while cleaning then the cleaning company could possibly not be held liable if the information is used for fraudulent purposes. Fifthly, a project to protect information throughout its lifecycle has not been implemented. This implies that information could be breached at various points of its lifecycle. Sixthly, employees are not regularly tested on information security policies. This implies that employees may not actually understand policies on security, and this increases the potential of

data breaches. Further conclusions reached are that information security is not comprehensively budgeted for by all areas of the organisation; instead, it is done in silos by certain areas. Better security management on 3<sup>rd</sup> party customer data transfer should be implemented, and the IT area should benchmark its security systems against international practises and guidelines. Overall, the results of this study shed light to the key factors to be considered by the organisation in relation to information-related aspects and therefore provides a solid foundation for the organisation to work off to improve the state of information management. Therefore, this study has improved the understanding of information management at the organisation as well as other similar organisations. The findings also contribute to the growing body of literature on information management in South Africa.

### **8.3 Recommendations for the organisation**

#### **8.3.1 Breaching of data in a financial institution**

This study recommends that skills development and training officers must conduct skills audits in relation to employees' knowledge of information management in order to create a centralised hub for training and skilling for this topic of information management. This will enable all employees across the organisation to understand the implications of data breaches and what their responsibilities are to stop data breaches. This training needs to include information on how data breaches affect the economic condition of the organisation, and employees should be trained on information management policies and procedures as opposed to just making the policies available. It is also recommended that the Data Governance Council (DGC) at the organisation conduct a business impact analysis in relation to information security in order to quantify risk management. This will further aid to achieve a comprehensive information security programme whereby all breaches of information are assessed. This study further recommends that the organisation appoint a fraud or data breach investigator to investigate internal data breaches. The data breaches should be split into two areas. The first would be accidental data breaches. These accidental data breaches should be sent to skills development and training officers who can incorporate action items into their training to educate and up-skill employees on data breaches. The second area is where employees purposefully violate information policies and guidelines with the purpose of harmful intentions. It is recommended that policy makers at the organisation standardise policies to ensure that these are applicable to all areas in the organisation. This is more applicable to house rules such as clean desk policies. All line managers across the organisation should ensure that all papers are removed and disposed of before employees end their shift. The clean desk policy should be part of the employee's tasks and, thus, part of the organisational guidelines for all departments. It is further recommended that all external cleaning staff at the organisation, or the cleaning company, sign a Non-Disclosure Agreement that states that all information found whilst cleaning is that of the financial institution and cannot be used by anyone else.



This does not prevent fraudulent activity but will give the financial institution in the study more legal leverage should fraud occur from this source.

### **8.3.2 Information management mitigation in a financial institution**

This study recommends that the DGC put in place a project to ensure personal information is protected from the moment it is created to the time it undergoes final disposition. It is also recommended under the dimension of information management mitigation that more training be done by the training department on information management as training can be more beneficial than just drafting policies that needs to be adhered to. Furthermore, it is recommended that trainers regularly test employees' knowledge of information security policies and guidelines.

### **8.3.3 Information management preparedness in a financial institution**

This study recommends that training officers at the organisation include preparedness plans on information management as part data breaching and information protection training. This training should include a set of procedures that employees follow if data breaches occur. Furthermore, it is recommended by this study that trainers and line managers at the organisation ensure that policies of information management are made clearer to employees who are to follow the policies. This could be done through various training programmes by the training office and re-capped by line managers through monthly meetings to keep policies in mind and promote accountability. In addition, this study recommends that monetary budgeting for information security form part of the annual budgeting process at the organisation. This should be done by all departments as all stakeholders need to be involved.

### **8.3.4 Information management systems in a financial institution**

This study recommends that stricter email control be placed on systems by the IT area. This is to allow customer information not to be passed to a 3<sup>rd</sup> party. It is further recommended that a more sophisticated access control system be set for when customer information needs to be sent or transferred for valid business related activities. This study further recommends that management in the IT area assess the IT security systems against internationally accepted standards and practises. In addition, the study recommends that all stakeholders in the business such as the heads of marketing, risk, collections, operations, finance and HR be involved when implementing IT systems as their needs could be different.

### **8.3.5 Risk response and recovery in a financial institution**

This study recommends that change management interventions takes place at the organisation in order for employees to proactively respond to data breaches. This could be done through firstly, risk assessments and analysis (as highlighted previously) and then be relayed to staff through training officers and line managers.

### **8.4 Limitations of the study**

There are some limitations to this study. The first limitation of the study is that the study set was limited to an organisation operating in South Africa. Caution, therefore, needs to be taken when generalising the results of the study. The second limitation is that only a few employees or respondents were in employ at the organisation in their current position for more than 3 years, which might limit the generalisability of the results. Furthermore, the organisation is a larger established institution; therefore, employees at smaller organisations may regard their security responsibilities as an additional duty than those of an established office, as depicted in the results of this study.

### **8.5 Guidelines for future researchers**

Future researchers investigating the study of information management could expand the research into other areas of the private sector where data sharing practises have been implemented. Furthermore, future researchers may want implement a modelled framework for any of the dimensions discussed in this research in order to provide a generic step by step model that organisations can implement on information security. In addition, future researchers should consider linking risk factors to both causes and consequences. It is believed that the results of the current study should provide future researchers with the rationale to continue to investigate the process, programmes and systems of information management in organisations. This study was performed prior to the operative sections of POPI coming into effect and it is recommended that an analysis similar to the one undertaken here be performed once POPI becomes effective.

## REFERENCES

- Abu-Musa, A. 2010. Information security governance in Saudi organizations: an empirical study. *Information Management and Security*, 18(4), 226-276.
- Ackers, B. & Eccles, N. S. 2015. Mandatory corporate social responsibility assurance practises: The case of King III in South Africa. *Accounting, Auditing and Accountability Journal*, 28(4), 515-550.
- Ahmad, A. & Maynard, S. 2014. Teaching information security management: Reflections and experiences. *Information Management and Computer Security*, 22(5), 513-536.
- Al-Mukahal, H.M. & Alshare, K. 2015. An examination of factors that influence the number of information security violations in Qatari organisations. *Information and Security*, 23(1), 102-118.
- Atkins, J. & Maroun, W. 2015. Integrated reporting in South Africa 2012. *Meditari Accounting Research*, 23(2), 197-221.
- Australian bureau of statistics. 2013. Census and sample. [ONLINE]. Available at: <http://www.abs.gov.au/websitedbs/a3121120.nsf/home/statistical+language+-+census+and+sample>. [Accessed 20 January 2016].
- Brennan, N. M. & Solomon, J. 2008. Corporate Governance, Accountability and Mechanisms of Accountability: An Overview. *Journal of Accounting and Audibility*, 21(7), 885-906.
- Bryman, A. 2006. Integrating quantitative and qualitative research: how it is done. *Journal of Qualitative Research*, 6(1), 77-113.
- Bulgurcu, B., Cavusoglu, H. & Benbasat, I. 2010. Information security compliance: An empirical study of rationality based beliefs and information security awareness. *Journal of Information security compliance*, 34(3), 523-548.
- Burmeister, B. 2014. Pay attention to the Protection of Personal Information Bill. *Finweek*, p. 7, Business Source Premier.
- Burns, N. & Grove, S. K. 2009. *Strategies for promoting evidence-based nursing practice in the practice of nursing research: Appraisal, synthesis and generation of evidence* (6th ed.). St. Louis: Saunders/Elsevier.
- Caldwell, F. 2008. Risk intelligence: Applying KM to information risk management. *Vine*, 38(2), 163-166.
- Chen, J., Pedrycz, W., Ma, L. & Wang, C. 2014. A new information security risk analysis method based on membership degree. *Kybernetes*, 43(5), 686-698.
- Chigamba, C. & Fatoki, O. 2011. Factors Influencing the Choice of Commercial Banks by University Students in South Africa. *International Journal of Business and Management*, 6(6), 66-76.
- Chikandiwa, S.T., Contogiannis, E. & Jembere, E. 2013. The adoption of social media marketing in South African banks. *European Business Review*, 25(4), 365-381.
- Chin, W.W., Johnson, N. & Schwars, A. 2008. A fast form approach to measuring technology acceptance and other constructs. *MIS Quarterly*, 32(4), 687-703.

- Choi, J.Y., Kim, Y., Jun, Y. & Kim, Y. 2011. A Bayesian multivariate probit analysis of Korean firms' information system adoption. *Industrial Management and Data Systems*, 111(9), 1465-1480.
- Clason, D. L. & Dormody, T. J. 1994. Analyzing data measured by individual Likert-type items. *Journal of Agricultural Education*, 35(4), 31- 35.
- Cliffe Dekker Attorneys, 2002. *King Report on Corporate Governance for South Africa*. [Online]. Available at: [http://www.mervynking.co.za/downloads/CD\\_King2.pdf](http://www.mervynking.co.za/downloads/CD_King2.pdf) [Accessed 16 August 2015].
- Cohen, L., Manion, L. & Morrison, K. 2007. *Research methods in education* (6<sup>th</sup> ed.). London: Routledge.
- Collin, C. 2009. Observations on the UK transformational government strategy relative to citizen data sharing and privacy. *Transforming Government: People, Process and Policy*, 3(4), 394-405.
- Collins, J.D., Sainato, V.A. & Khey, D.N. 2011. Organizational Data Breaches 2005-2010: Applying SCP to the Healthcare and Education Sectors. *International Journal of Cyber Criminology*, 5(1), 794-810.
- Collins, J. & Hussey, R. 2009. *Business Research: A practical guide for undergraduate and postgraduate students* (3<sup>rd</sup> ed.). Hampshire, U.K: Palgrave Macmillan.
- Combe, C. 2009. Observations on the UK transformational government strategy relative to citizen data sharing and privacy. *Transforming Government: People, Process and Policy*, 3(4), 394-405.
- Cooper, D.R. & Schindler, P.S. 2003. *Business Research methods* (8<sup>th</sup> ed.) Boston: McGraw-Hill.
- Creswell, J. W. 2003. *Research design: Qualitative, quantitative and mixed methods approaches* (2<sup>nd</sup> ed.). London: Sage Publications.
- Cullen, R. 2009. Culture, identity and information privacy in the age of digital government. *Online Information Review Journal*, 33(3), 405-421.
- D'Arcy, J. & Greene, G. 2014. Security culture and the employment relationship as drivers of employees' security compliance. *Information Management and Computer Security*, 22(5), 474-489.
- Desai, M.S., Desai, K.J. & Phelps, L.D. 2012. E-commerce policies and customer privacy: a longitudinal study (2000-2010). *Information Management and Computer Security*, 20(3), 222-244.
- Department of Trade and Industry. 2009. *The Consumer Protection Act: Your guide to consumer rights and how to protect them*. [ONLINE]. Available at: [https://www.westerncape.gov.za/other/2011/3/consumer\\_protection\\_act.pdf](https://www.westerncape.gov.za/other/2011/3/consumer_protection_act.pdf). [Accessed 22 August 2015].
- Desai, M.S. & von der Embse, T.J. 2008. Managing electronic information: an ethics perspective. *Information Management and Computer Security*, 16(1), 20-27.

- Doody, O. & Noonan, M. 2013. Preparing and conducting interviews to collect data. *Nurse Researcher*, 20(5), 28-32.
- Efraimidis, P.S., Drosatos, G., Nalbadis, F. & Tasidou, A. 2009. Towards privacy in personal data management. *Information Management & Computer Security*, 17(4), 311-329.
- Ehlers, T. & Lazenby, K. 2010. *Strategic Management: South African Concepts and Cases* (3<sup>rd</sup> ed.). Pretoria: Van Schaik.
- Fenz, S., Heurix, J., Neubauer, T. & Pechstein, F. 2014. Current challenges in information security risk management. *Information Management and Computer Security*, 22(5), 410-430.
- Fisher, J.A. 2013. Secure My Data or Pay the Price: Consumer Remedy for the Negligent Enablement of Data Breach. *William and Mary Business Law Review*, 4(1), 215-239.
- Fourie, I. 2011. Personal information and reference management: Librarians increasing productivity. *Library Hi Tech*, 29(2), 387-393.
- Fox, A. & Ritchie, E. (n.d), Ethical Research Guidelines for Staff and Students, Faculty of Arts and Architecture, University of Brighton.
- Fraenkel, J.R. & Wallen, N.E. 2000. *How to design and evaluate research in education*. London: McGraw Hill.
- Frangopoulos, E. D., Eloff, M.M. & Venter, L. M. 2013. Psychological risks. *Information Management and Computer Security*, 21(1), 53-65.
- Gable, J. 2014. Principles for protecting information privacy. *Information Management Journal*, 48(5), 38-42.
- Gal, U. & Berente, N. 2008. A social representations perspective on information systems implementation. *Information Technology and People*, 21(2), 133-154.
- Garrison, C.P. & Ncube, M. 2011. A longitudinal analysis of data breaches. *Information Management and Computer Security*, 19(4), 216-230.
- Gordon, L.A., Martin, P.L. & Zhoe, L. 2011. The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security*, 19, 33-56.
- Gupta, P. 2012. Risk management in networked information system. *Journal of System Security*, 3(1), 241-245.
- Gonzalez, R., Gasco, J. & Llopis, J. 2010. Information systems outsourcing reasons and risks: a new assessment. *Industrial Management and Data Systems*, 111(2), 284-303.
- Hagmann, J. 2013. Information governance – beyond the buzz. *Records Management Journal*, 23(3), 228-240.
- Hagen, J.M. & Albrechtsen, E. 2009. Effects on employees' information security abilities by e-learning. *Information Management and Computer Security*, 17(5), 388-407.
- Hausmann, R., Tyson, L. D. & Zahidi, S. 2009. *The global Gender Gap Report*. Geneva: World Economic Forum.

- Haneef, S., Riaz, T., Ramzan, M., Rana, M. A., Ishaq, H. M. & Karim, Y. 2012. Impact of Risk Management on Non-Performing Loans and Profitability of Banking Sector of Pakistan. *International Journal of Business and Social Science*, 3(7), 307-315.
- Heppes, D. & du Toit, A. 2009. Level of maturity if the competitive intelligence function: case study of a retail bank in South Africa. *Aslib Proceedings*, 61(1), 48-66.
- Herath, T. & Rao, H. R. 2009. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Journal of Decision Support Systems*, 47, 154-165.
- Hertel, G., Van der Heijden, B. I. J. M., de Lange A, H. & Deller, J. 2009. Facilitating age diversity in organizations – part II: managing perceptions and interactions. *Journal of Managerial Psychology*, 28(7/8), 857-866.
- Holloway, I. 1997. *Basic concepts for qualitative research*. Abingdon: Blackwell Science.
- Holtfreter, R. & Harrington, A. 2015. Data breach trends in the United States. *Journal of Financial Crime*, 22(2), 242-260.
- Jarvelainen, J. 2012. Information security and business continuity management in Inter-organisational IT relationships. *Information management and Computer Security*, 20(5), 332-349.
- Jianping, C. & Zhongwei, Y. 2009. The characteristics and enlightenment of legislation on financial privacy protection in the USA. *International Journal of Law and Management*, 51(4), 226-233.
- Johnston, A.C. & Warkentin, M. 2008. Information privacy compliance in the healthcare industry. *Information Management and Computer Security*, 16(1), 5-19.
- Kahraman, C., Kaya, I. & Cevikcan, E. 2011. Intelligence decision systems in enterprise information management. *Journal of Enterprise Information Management*, 24(4), 360-379.
- Katos, V. & Patel, A. 2008. A partial equilibrium view on security and privacy. *Information Management and Computer Security*, 16(1), 74-83.
- Katuu, S. 2012. Enterprise content management implementation in South Africa. *Records Management Journal*, 22(1), 37-56.
- Kieke, R. L. 2014. Recent data breach stresses the importance of effective privacy efforts. *Journal of Health Care Compliance*, 16(1), 45-50.
- King, B. & Thatcher, A. 2012. Attitudes towards software piracy in South Africa: Knowledge of Intellectual Property Laws as a moderator. *Direct Marketing: Behaviour and Information Technology Journal*, 33(3), 209-223.
- Knapp, K. J., Morris, R, F., Marshall, T, E. & Byrd, T. A. 2009. Information security policy: An organizational-level process model. *Journal of Computers and Security*, 1-16.
- Ko, D. & Fink, D. 2010. Information technology governance: an evaluation of the theory practice gap. *Journal of Corporate Governance*, 10(5), 662-674.

- Kosciejew, M. 2014. Proposing a Charter of Personal Data Rights. *Information Management Journal*, 48(3), 27-31.
- KPMG. 2013. *A practical response to POPI*. [ONLINE]. Available at: <http://www.kpmg.com/ZA/en/IssuesAndInsights/ArticlesPublications/Protection-of-Personal-Information-Bill/Documents/Practical%20Response%20to%20POPI-final.pdf>. [Accessed 12 October 2014].
- Lacey, D. 2010. Understanding and transforming organizational security culture. *Information Management and Computer Security*, 18(1), 4-13.
- Luker, K. 2008. *Salsa dancing into the social sciences – research in an age of info-glut*. Cambridge: Harvard University Press.
- Malhotra, A. & Malhotra, C. K. 2011. Evaluating Customer Information Breaches as Service Failures: An Event Study Approach. *Journal of Service Research*, 14(1), 44-59.
- Malmir A. & Malmir, M. 2015. Government's civil liability towards individuals' privacy in cyberspace. *International Journal of Law and Management*, 57(2), 98-106.
- Marshal, R., Cardon, P., Poddar, A. & Fontenot, R. 2013. Does sample size matter in qualitative research? A review of qualitative interviews in IS research. *Journal of Computer Information Systems*, 54(1), 11-22.
- Marx, B. & van Dyk, V. 2011. Sustainability reporting and assurance: an analysis of assurance practices in South Africa. *Meditari Accountancy Research*, 19(1/2), 39-55.
- McMillian, J. & Schumacher, S. 2008. *Research in education: Evidence-based inquiry* (6<sup>th</sup> ed.). Boston: Pearson.
- Moghavvemi, S. & Salleh, N.A.M. 2014. Effect of precipitating events on information system adoption and use behaviour. *Journal of Enterprise Information Management*, 27(5), 599-622.
- Morse, J. M., Barret, M., Mayan, M., Olson, K. & Spiers, J. 2002. Verification Strategies for Establishing Reliability and Validity in Qualitative Research. *Journal of Qualitative Methods*. 1(2), 13-22.
- Murata, K. & Orito, Y. 2008. Rethinking the concept of the right to information privacy: a Japanese perspective. *Journal of Information, Communication and Ethics in Society*, 6(3), 233-245.
- Mutula, S. & Kaloate, T. 2010. Open source software development in the public sector: a review of Botswana and South Africa. *Library Hi Tech*, 28(1), 63-80.
- Mutula, S.M. & Mostert, J. 2010. Challenges and opportunities of e-government in South Africa. *The Electronic Library*, 28(1), 38-53.
- Nazimoglu, O. & Ozsen, Y. 2010. Analysis of risks dynamics in information technology service delivery. *Journal of Enterprise Information Management*, 23(3), 350-364.
- Neelankavil, J.P. 2007. *International business research*. New York: Library of Congress Cataloging-in-Publication Data.

- Niessen, C., Swarowsky, C. & Leiz, M. 2010. Age and adaption to changes in the workplace. *Journal of Managerial Psychology*, 25(4), 356-383.
- Nieuwenhuis, J. 2007. *Qualitative research designs and data gathering techniques*. In Maree, K. (ed). *First Steps in Research*, pp. 70-97. Pretoria: Van Schaik.
- Ngoepe, M. & Makhubela, S. 2015. Justice delayed is justice denied. *Records Management Journal*, 25(3), 288-305.
- Oppenheim, A.N. 2000. *Questionnaire Design, Interviewing and Attitude Measurement*. New York: Basic Books.
- O'Rourke, N. & Hatcher, L. 2013. *A step-by-step approach to using SAS for factor analysis and structural equation modelling* (2<sup>nd</sup> ed.). North Carolina: SAS Institute Inc.
- Otapah, F.O. & Dadzie, P. 2013. Personal information management practices of students and its implications for library services. *Aslib Proceedings*, 65(2), 143-160.
- Pawar, M. 2004. *Data Collecting Methods and Experiences: A Guide for Social Researchers*. New Delhi: New Dawn Press Group.
- Peters, M, L. & Zelewski, S. 2007. Assignment of employees to workplaces under consideration of employee competences and preferences. *Management Research News*, 30(2), 84-99.
- Pike, G. 2009. Congress debates data breach legislation. *Information Today*, 26(11), 17-19.
- Polonski, M.J. & Waller, D.S. 2010. *Designing and Managing a Research Project: a business student's guide*. California: Sage Publications.
- Pope, J.A. & Lowen, A.M. 2009. Marketing implications of privacy concerns in the US and Canada. *Direct Marketing: An international Journal*, 3(4), 301-326.
- Relly, J. E. & Sabharwal, M. 2008. Perceptions of transparency of government policymaking: A cross-national study. *Government Information Quarterly*. 26. 148-157.
- Rooney, J. & Cuganesan, S. 2015. Leadership, governance and the mitigation of risk: a case Study. *Managerial Auditing Journal*, 30(2), 132-159.
- Rossouw, G. J., van der Watt, A. & Malan, D. P. 2002. Corporate Governance in South Africa. *Journal of Business Ethics*, 37(3), 289-302.
- Ruane, J.M. 2004. *Essentials of research methods: A guide to social research*. London: Wiley-Blackwell.
- Sampson, H. 2004. Navigating the waves: the usefulness of a pilot in qualitative research. *Qualitative Research*, 4(3), 383-402.
- Saunders, M., Lewis, P. & Thornhill, A. 2000. *Research Methods for Business Students*. Essex: Financial Times Prentice Hall.
- Shedden, P., Scheepers, R., Smith, W. & Ahmad, A. 2011. Incorporating a knowledge perspective into security risk assessments. *Vine*, 41(2), 152-166.



- Shropshire, J. 2009. A canonical analysis of intentional information security breaches by insiders. *Information Management and Computer Security*, 17(4), 296-310.
- Siddiqui, J. 2010. Development of Corporate Governance Regulations: The Case of an Emerging Economy. *Journal of Business Ethics*, 91, 253-274.
- Silverman, D. 2010. *Doing qualitative research*. London: Sage.
- Singh, A. N., Gupta, M.P. & Ojha, A. 2014. Identifying factors of organisational information security management. *Journal of Enterprise information Management*, 27(5), 644-667.
- Smith, H, J., Dinev, T. & H, Xu. 2011. Information privacy research: An interdisciplinary review. *MIS Quarterly*, 35(4), 989-1015.
- South Africa. 2000. *Promotion of Access to Information Act, No.2 of 2000*. [ONLINE]. Available at: <http://www.justice.gov.za/legislation/acts/2000-002.pdf>. [Accessed 22 August 2015].
- South Africa. 2008. Consumer Protection Act, No. 68 of 2008. [ONLINE]. Available at: <http://www.justice.gov.za/legislation/acts/2008-068.pdf>. [Accessed 22 August 2015].
- South Africa. 2013. *Protection of Personal Information Act, No.4 of 2013*. [ONLINE]. Available at: <http://www.justice.gov.za/legislation/acts/2013-004.pdf>. [Accessed 09 October 2014].
- Stewart, A. 2012. Can spending on information security be justified – Evaluating the security spending decision from the perspective of a rational actor. *Information Management and Computer Security*. 20(4), 312-326.
- Strauss, A.C. & du Toit, A.S.A. 2008. Competitive intelligence skills needed to enhance South Africa's competitiveness. *Aslib Proceedings*, 62(3), 302-320.
- Sujatha, R. 2011. An Analysis of Text-Based Authentication using Images in Banking System. *Journal of Computer Engineering and Intelligent Systems*, 2(4), 136-148.
- Sumanjeet, D. 2010. The state of e-commerce laws in India: a review of Information Technology Act. *International Journal of Law and Management*, 52(4), 265-282.
- Teddlie, C. & Yu, F. 2007. Mixed method sampling: A typology with examples. *Journal of Mixed Method Research*, 1(1), 77-100.
- Thomson, K. & van Niekerk, J. 2012. Combating information security apathy by encouraging prosocial organisational behaviour. *Information Management and Computer Security*. 20(1), 39-46.
- Trochim, W.M.K. 2006. Non-probability sampling. [ONLINE]. Available at: <http://www.socialresearchmethods.net/kb/samprnon.php>. [Accessed 19 January 2016].
- Tsohou, A., Kokolakis, S., Lambrinouidakis, C. & Gritzalis, S. 2010. A security standards framework to facilitate best practices awareness and conformity. *Information Management and Computer Security*, 18(5), 350-365.
- Van Niekerk, J.F. & Van Solms, R. 2010. Information security culture: A management perspective. *Journal of Computers and Security*, 29, 476-486.

- Verhofstadt, E., De Witte, H. & Omey, E. 2007. Higher educated workers: better jobs but less satisfied. *International Journal of Manpower*, 28(2), 135-151.
- Wessels, L. 2000. *The guide on how to use the Promotion of Access to Information Act – Act 2 of 2000*. [ONLINE]. Available at: <http://www.dfa.gov.za/department/paia.pdf>. [Accessed 22 August 2015].
- West, A. 2009. The ethics of corporate governance: A South African perspective. *International Journal of Law and Management*, 51(1), 10-16.
- Willenweber, K., Jahner, S. & Krcmar, H. 2008. *Relational risk mitigation: The relationship approach to mitigating risks in business process outsourcing*. Available at: <http://www.krcmar.informatik.tu-muenchen.de/publikat.nsf/.pdf>. [Accessed 14 April 2015].
- Yin, R. K. 2011. *Qualitative research from start to finish*. New York: Guilford Press.
- Young, L. 2010. Data Protection – Specification for a Personal Information Management System. *Records Management Journal*. 20(1). Zaman, M. n.d. *Predictive Analytics: The Future of Business Intelligence*. Available at: [https://scholar.google.co.za/scholar?start=10&q=SPSS+analytics&hl=en&as\\_sdt=0,5](https://scholar.google.co.za/scholar?start=10&q=SPSS+analytics&hl=en&as_sdt=0,5). [Accessed 14 April 2015].
- Zhang, J., Reithel, B.J. & Li, H. 2009. Impact of perceived technical protection on security behaviors. *Information Management and Computer Security*, 17(4), 330-340.
- Zhou, L., Vasconcelos, A. & Nunes, M. 2008. Supporting decision making in risk management through an evidence-based information systems project risk checklist. *Information Management and Computer Security*, 16(2), 166-186.
- Zwikaël, O. 2008. Top management involvement in project management. *International Journal of Managing Projects in Business*, 1(3), 387-403.

## APPENDIX A: STRUCTURED QUESTIONNAIRE

SUPERVISOR DETAILS	
Name:	Bethuel
Surname:	Ngcamu
Email:	Ngcamub@cput.ac.za

RESEARCH TITLE
An empirical investigation into the information management systems at a South African financial institution.
PURPOSE AND IMPACT OF STUDY
<p>The study has been triggered by the increase in information breaches in organisations. Organisations may have policies and procedures, strategies and systems in place in order to mitigate the risk of information breaches but the data breaches are still on the rise. Governments across the world have or are putting in place laws around data protection which organisations have to align their process, strategies and systems to.</p> <p>Organisational compliance on information is a topical issue that impacts many organisations. Many of these organisations have not fully come to grip with the actual implications to the business or understand how employees are dealing with this on a day to day basis. The research is important as it will assist a selected financial institution to fill a gap in the ability to handle information management in the organisation. As highlighted previously, there are many aspects of information which companies have to cater for such as government legislation and company policies as well as marrying these two up.</p>

HOW TO COMPLETE THIS SURVEY
<ul style="list-style-type: none"> <li>➤ This survey mostly comprises of close ended questions which requires the respondent to mark an 'x' in the appropriate column or tick box.</li> <li>➤ Clear instructions for each question are given under each section.</li> <li>➤ If you do not understand the question please feel free to contact the researcher and/or supervisor indicated on the front page.</li> </ul>

CONFIDENTIALITY AND ANONYMITY
Please note that ALL information provided by any respondent will be kept strictly confidential and the anonymity of the respondent is guaranteed.

SECTION A – BIOGRAPHICAL INFORMATION		
<b>1) Gender (Make an 'x' in the appropriate box)</b>		
Male	<input type="checkbox"/>	<input type="checkbox"/>
Female	<input type="checkbox"/>	<input type="checkbox"/>
<b>2) Age (Make an 'x' in the appropriate box)</b>		
21-30	01	<input type="checkbox"/>
31-40	02	<input type="checkbox"/>
41-50	03	<input type="checkbox"/>
51-60	04	<input type="checkbox"/>
60-65	05	<input type="checkbox"/>
65 and above	06	<input type="checkbox"/>
<b>3) Highest level of education completed (Make an 'x' in the appropriate box)</b>		
Below matric	01	<input type="checkbox"/>
Matric	02	<input type="checkbox"/>
Diploma	03	<input type="checkbox"/>
Bcom or Btech	04	<input type="checkbox"/>
Honours	05	<input type="checkbox"/>
Masters	06	<input type="checkbox"/>
PhD	07	<input type="checkbox"/>
<b>4) What staffing level can you be classified in? (Make an 'x' in the appropriate box)</b>		
Executive Management	01	<input type="checkbox"/>
Senior Management	02	<input type="checkbox"/>
Middle Management	03	<input type="checkbox"/>
Non Managerial Specialist	04	<input type="checkbox"/>
Lower Level Management	05	<input type="checkbox"/>
Agent Level	06	<input type="checkbox"/>
<b>5) Area of Specialisation</b>		
Collections	01	<input type="checkbox"/>
Compliance/Legal	02	<input type="checkbox"/>
Credit Risk	03	<input type="checkbox"/>
Finance	04	<input type="checkbox"/>
Information Technology	05	<input type="checkbox"/>
Human Resources	06	<input type="checkbox"/>
Marketing	07	<input type="checkbox"/>
Operations	08	<input type="checkbox"/>
Other	09	<input type="checkbox"/>
If other, please specify: _____		
<b>6) How long have you been in this position at the company? (Make an 'x' in the appropriate box)</b>		
0 to 3 years	01	<input type="checkbox"/>
4 to 6 years	02	<input type="checkbox"/>
7 to 10 years	03	<input type="checkbox"/>
More than 10 years	04	<input type="checkbox"/>

**SECTION B – BREACHING OF DATA IN A FINANCIAL INSTITUTION**

Answer the following questions by making an 'x' in the appropriate number [1 = strongly disagree, 2 = disagree, 3 = undecided, 4 = agree, 5 = strongly agree]

**In my institution:**

7) I ensure that I do not breach confidential information	1	2	3	4	5
8) I ensure that I secure organisational personal information	1	2	3	4	5
9) I make sure that I don't breach security information	1	2	3	4	5
10) I'm not associated in fraudulent activities	1	2	3	4	5
11) My activities are aligned to government regulations	1	2	3	4	5
12) There are no occurrences of information breaches	1	2	3	4	5
13) Data breaches has a positive impact	1	2	3	4	5
14) Customers are not concerned about information management	1	2	3	4	5
15) Breaching of information is assessed	1	2	3	4	5
16) Employees are trained on information security policies	1	2	3	4	5
17) Experienced employees are more compliant on security policies	1	2	3	4	5
18) Employees keep customer information confidential	1	2	3	4	5
19) Employees are held accountable for breaching customer data	1	2	3	4	5
20) Data breaches do not affect its economic condition	1	2	3	4	5
21) Data breaches only occur accidentally	1	2	3	4	5

**SECTION C – INFORMATION MANAGEMENT MITIGATION IN A FINANCIAL INSTITUTION**

Answer the following questions by making an 'x' in the appropriate number [1 = strongly disagree, 2 = disagree, 3 = undecided, 4 = agree, 5 = strongly agree]

**In my institution:**

22) Information management security policies are in place	1	2	3	4	5
23) Information management programmes are in place to educate employees	1	2	3	4	5
24) There is low risk of information breaches	1	2	3	4	5
25) Information is protected from the moment it is created until the end of its cycle	1	2	3	4	5
26) I have access to customer information that is not a necessity to perform my job	1	2	3	4	5
27) I have attended information management training which is beneficial to me	1	2	3	4	5
28) Information management risks are managed well	1	2	3	4	5
29) Risk assessments are done in order to quantify threats	1	2	3	4	5
30) Management plays an important role to promote information security	1	2	3	4	5
31) Money is spent to mitigate data breaches	1	2	3	4	5
32) Information security is part of my organisational culture	1	2	3	4	5
33) There are awareness campaigns on information security	1	2	3	4	5
34) Employees' knowledge is regularly tested on information security policies and procedures	1	2	3	4	5

**SECTION D – INFORMATION MANAGEMENT PREPAREDNESS IN A FINANCIAL INSTITUTION**

Answer the following questions by making an 'x' in the appropriate number [1 = strongly disagree, 2 = disagree, 3 = undecided, 4 = agree, 5 = strongly agree]

**In my institution:**

35) I am aware of government regulations and procedures on information management	1	2	3	4	5
36) Employees are the strongest link in information security	1	2	3	4	5
37) If data breaches do occur there is a set procedures in place that I will follow	1	2	3	4	5
38) Information management security is part of my institutional culture	1	2	3	4	5
39) Policies on information management are clear	1	2	3	4	5
40) There are disciplinary measures in place to address employee negligence on information management	1	2	3	4	5
41) Information security forms part of the annual organisations budgeting	1	2	3	4	5

**SECTION E – INFORMATION MANAGEMENT SYSTEMS IN A FINANCIAL INSTITUTION**

Answer the following questions by making an 'x' in the appropriate number [1 = strongly disagree, 2 = disagree, 3 = undecided, 4 = agree, 5 = strongly agree]

**In my institution:**

42) Technology based solutions are all that is required to ensure information security	1	2	3	4	5
43) Without IT systems we cannot control information management	1	2	3	4	5
44) The software systems I use have strict access control to customer information	1	2	3	4	5
45) The IT systems are aligned with the requirements of protecting customer information	1	2	3	4	5
46) Data protection and security protection controls are in place on computers	1	2	3	4	5
47) Employees have access to pass customer information to a third party. E.g. via email	1	2	3	4	5
48) All interactions with customers are recorded on an IT system	1	2	3	4	5
49) The IT area is well informed of necessities related to privacy regulation and policies	1	2	3	4	5
50) The standard of information security systems are assessed against international accepted rules and practises	1	2	3	4	5
51) Employees are required to demonstrate to consumers their level of compliance in relation to information security guidelines	1	2	3	4	5
52) All business stakeholders are involved when implementing IT systems	1	2	3	4	5
53) Information systems are becoming more exposed to risk and breaches	1	2	3	4	5

**SECTION F – RISK RESPONSE AND RECOVERY IN A FINANCIAL INSTITUTION**

Answer the following questions by making an 'x' in the appropriate number [1 = strongly disagree, 2 = disagree, 3 = undecided, 4 = agree, 5 = strongly agree]

**In my institution:**

54) Information risk management is not important	1	2	3	4	5
55) Risk management does not need to form part of a business strategy	1	2	3	4	5
56) The requirement for risk management is on the decrease	1	2	3	4	5
57) Regulatory risks should not form part of the institution's risk plan	1	2	3	4	5
58) There are no controls in place to react to information management risks	1	2	3	4	5
59) We do not respond well to risks on information management	1	2	3	4	5
60) There are no contingency plans in place to deal with risks on information management	1	2	3	4	5
61) Information is not securely backed up in the event it should be lost	1	2	3	4	5
62) I am not able to identify information risks	1	2	3	4	5
63) I reactively respond to information risks	1	2	3	4	5
64) There are instances when I do not get notifications on information risks	1	2	3	4	5

Would you like e-mail feedback of this study?	
Yes	No
Email address:	

## APPENDIX B: SEMI STRUCTURED IN-DEPTH INTERVIEWS

### Interview 1:

SUPERVISOR DETAILS	
Name:	Bethuel
Surname:	Ngcamu
Email:	Ngcamub@cput.ac.za

RESEARCH TITLE
An empirical investigation into the information management systems at a South African financial institution.
PURPOSE AND IMPACT OF STUDY
<p>The study has been triggered by the increase in information breaches in organisations. Organisations may have policies and procedures, strategies and systems in place in order to mitigate the risk of information breaches but the data breaches are still on the rise. Governments across the world have or are putting in place laws around data protection which organisations have to align their process, strategies and systems to.</p> <p>Organisational compliance on information is a topical issue that impacts many organisations. Many of these organisations have not fully come to grip with the actual implications to the business or understand how employees are dealing with this on a day to day basis. The research is important as it will assist a selected financial institution to fill a gap in the ability to handle information management in the organisation. As highlighted previously, there are many aspects of information which companies have to cater for such as government legislation and company policies as well as marrying these two up.</p>

HOW TO COMPLETE THE INTERVIEW AND THE TARGET POPULATION
<ul style="list-style-type: none"> <li>➤ This interview questions comprises of open-ended questions which requires the respondent to verbally respond to the questions.</li> <li>➤ The interview questions are aimed at executive management in the organisation.</li> <li>➤ The questions will be asked face to face by the researcher. If the question is not understood the researcher will be on hand to explain the question.</li> <li>➤ The researcher will document all answers to the questions represented on this interview question list.</li> </ul>

CONFIDENTIALITY AND ANONYMITY
Please note that ALL information provided by any respondent will be kept strictly confidential and the anonymity of the respondent is guaranteed.

SECTION A – BIOGRAPHICAL INFORMATION	
<b>1) Gender</b>	
Male	01X
Female	02
<b>2) Age</b>	
21-30	01
31-40	02
41-50	03X
51-60	04
60-65	05
65 and above	06
<b>3) Highest level of education completed</b>	
Below matric	01
Matric	02
Diploma	03
Bcom or Btech	04
Honours	05X
Masters	06
<b>4) What staffing level can you be classified in?</b>	
Executive Management	01X
Senior Management (Non Executive)	02
<b>5) What is your current job title?</b>	
Head of Data	
<b>6) How long have you been in this position at the company?</b>	
0 to 3 years	01X
4 to 6 years	02
7 to 10 years	03
More than 10 years	04

**7) What plans do you have to ensure that employees do not breach information in this organisation?**

I'll focus on data breaches that is my key focus. So we have a system, well the control that we have is a Data Governance Council (DGC) and through data governance we make sure that all the policies and procedures are rolled out and then there's ownership within each line of business. There's certain policies and procedures defined around data breaches and that's how governed. It's also easier to make changes as it's rolled out to all the different data stewards to implement. So from a data breach point of view there's regulatory changes all the time with legislation so it comes through compliance projects and the way that we deal with that is through our EPO (Enterprise Project Office) process. So I will put a business concept document together for changes. We will then approve the project at executive level, so what is the priority. We will then deliver it to the EPO so that's kind of you how you maintain and change all the systems and anything related to data privacy and data security. This is kind of the two areas. So there's a lot of regulations to work through at the moment that we busy with at the moment.

**8) Do you have policies in this institution dealing with information management?**

**YES/NO**

Yes.

**If YES, are they responsive or aligned to the national legislations?**

Yes, where it's new or there are amendments we are busy planning through projects to change that.

**What are the opportunities and challenges brought by this policy?**

Absolutely, so legislation in South Africa around just about the entire finance system is very vast compared to first world countries. So governance in the financial sector is probably over-governed. There's so much regulation. We have challenges at the moment where we have NCAA (National Credit Act Amendment), there's POPI (Protection of Personal Information Act), there's a lot that have elements of data privacy and data security built into it. So what is the challenge? The volumes. The volumes of the changes and regulatory changes and accommodating them all the time because you also need to run your normal business and it competes because you want to make product enhancements, you want to run initiatives to enhance revenue and they compete. So every time you deal with compliance and regulatory

changes you kind of keep yourself as business back. So that's the biggest challenge is kind of to fit it in and deal with opportunities that you lose as you can only do so much.

**If NO/YES, what are your organizational plans in place to ensure that your key stakeholders (employees and vendors etc.) do not breach information?**

Your biggest control is your third party contract. Within the contract it specifies all your different clauses to say what to do with your data. We have the challenge that a lot of the contracts was put in place before the DGC, before we took a good look. We trying to identify those. We'll probably have to re-contract them but that is kind of your biggest control is to make sure all your rules and regulations are defined in your contract.

**What tools do you have in place to ensure that your key stakeholders do not breach information?**

Contracts is the biggest control.

## **SECTION C – INFORMATION MANAGEMENT MITIGATION IN A FINANCIAL INSTITUTION**

**9) Do you have in this organization mitigation strategies on information management?**

**YES/NO**

Absolutely.

**10) What are your mitigation plans in relation to information management?**

All of those are embedded in your BCP (Business Continuity Planning) and BR (Business Risk) processes. Well not all of them, but that's first and foremost. If there is a problem we'll deal with them through that. If there is a breach of information that's where our compliance and legal area will get involved in. My role in all of that is to make sure that if maybe there is a control missing or maybe there's a problem in a system to deal with it and maybe it's something we not dealing with in the policies we can put that in place. If there is a breach for whatever reason compliance and legal will also have to deal with it.

**11) Are staff members, other than executive management, aware and knowledgeable of the information management security policies put in place by the organisation? YES/NO**

Yes.

**a) If yes, what is done in order to achieve this?**



It will never be at a level that you want it to be but it starts from the day that you walk into the business. There's an employment contract and within the employment contract there's policies and procedures that you sign and then changes are communicated via HR. All communication that compliance will put together or IT will put together so it's there but you always want it at a higher level

**b) If no, what does the organisation view as the being important in relation to information management?**

#### **SECTION D – INFORMATION MANAGEMENT PREPAREDNESS IN A FINANCIAL INSTITUTION**

**12) Do you have preparedness plans to respond to any potential risk on information management? YES/NO**

There's definitely a process. The process will ensure that there's plan in place to kind of analyse the recourse and make sure it's covered. It's through our ITRC which is our Information Technology Risk Committee. It will be logged there and it will be driven through whoever the stakeholder is that's involved. They need to come up with a plan they need to come up with ownership, they will deal with it that way. So plan and process, yes.

**a) How are government policies and regulations on information management aligned with this organisations policies?**

It's done through planning of projects and getting it signed off at executive level.

**b) If it's not aligned, what are the organisations view on the future state to align this?**

#### **SECTION E – INFORMATION MANAGEMENT SYSTEMS IN A FINANCIAL INSTITUTION**

**13) How are the organisations technology systems aligned to the strategic plans of the organisation in relation to information management?**

That's a difficult question because it's difficult to look at information systems within administrators of the organisation but it plays a massive part. If the strategy is to take a new product to market there'll be a big portion of it talking to the development of the system and you will drive it through

process. If the strategy is approved at the highest level it won't talk to information systems it will say new product, new market that you want to achieve. For instance you want to go into offshore or you want to take new product. That will be a clue. Then we will do a business case. The business case will be approved and then we have to unpack it into business owners and that will then need system changes. Sometimes there could be information system driven strategy and that is major enhancements to systems that you need. We call it Eskom type projects. You have WIGs (Wildly Important Goals), this is business owned but we will also come back and say we need to replace a system its past its sell buy date and then there'll be strategy. Most of the strategies talk to business needs and we will then align the system components.

**a) If it's not aligned, why?**

**SECTION F – RISK RESPONSE AND RECOVERY IN A FINANCIAL INSTITUTION**

**14) What are the organisations risk management plans to deal with information management breaches?**

I'm really the wrong person to answer that question. The operational risk manager is probably the best to talk through that as we'll rely on him to deal with that and deal with the key stakeholders and put plans together. From my point of view there may be a piece of work allocated to me through that process then I will drive it. Exactly how that works is probably best to speak to operational risk manager.

I'm busy putting a third part data register together to make sure we know exactly who's got access to our data, what's the frequency, what is the ETL (Extract Transform and Load) process, does it conform to our needs.

It's an information driven organization so it's serious if there's a breach but then IT also have certain policies and procedures.

## Interview 2:

SUPERVISOR DETAILS	
Name:	Bethuel
Surname:	Ngcamu
Email:	Ngcamub@cput.ac.za

RESEARCH TITLE
An empirical investigation into the information management systems at a South African financial institution.
PURPOSE AND IMPACT OF STUDY
<p>The study has been triggered by the increase in information breaches in organisations. Organisations may have policies and procedures, strategies and systems in place in order to mitigate the risk of information breaches but the data breaches are still on the rise. Governments across the world have or are putting in place laws around data protection which organisations have to align their process, strategies and systems to.</p> <p>Organisational compliance on information is a topical issue that impacts many organisations. Many of these organisations have not fully come to grip with the actual implications to the business or understand how employees are dealing with this on a day to day basis. The research is important as it will assist a selected financial institution to fill a gap in the ability to handle information management in the organisation. As highlighted previously, there are many aspects of information which companies have to cater for such as government legislation and company policies as well as marrying these two up.</p>

HOW TO COMPLETE THE INTERVIEW AND THE TARGET POPULATION
<ul style="list-style-type: none"> <li>➤ This interview questions comprises of open-ended questions which requires the respondent to verbally respond to the questions.</li> <li>➤ The interview questions are aimed at executive management in the organisation.</li> <li>➤ The questions will be asked face to face by the researcher. If the question is not understood the researcher will be on hand to explain the question.</li> <li>➤ The researcher will document all answers to the questions represented on this interview question list.</li> </ul>

CONFIDENTIALITY AND ANONYMITY
Please note that ALL information provided by any respondent will be kept strictly confidential and the anonymity of the respondent is guaranteed.

SECTION A – BIOGRAPHICAL INFORMATION	
<b>1) Gender</b>	
Male	01X
Female	02
<b>2) Age</b>	
21-30	01
31-40	02X
41-50	03
51-60	04
60-65	05
65 and above	06
<b>3) Highest level of education completed</b>	
Below matric	01
Matric	02
Diploma	03
Bcom or Btech	04
Honours	05
Masters	06X
<b>4) What staffing level can you be classified in?</b>	
Executive Management	01
Senior Management (Non Executive)	02X
<b>5) What is your current job title?</b>	
Business Centre Leader: Operational Risk	
<b>6) How long have you been in this position at the company?</b>	
0 to 3 years	01X
4 to 6 years	02
7 to 10 years	03
More than 10 years	04

**7) What plans do you have to ensure that employees do not breach information in this organisation?**

If you viewing from the position that information is an asset and that we need to look after it then we've got a number of steps that we take to make sure that the information doesn't leak. I'm not going to specifically speak to a POPI (Protection of Personal Information Act) perspective now because POPI is not yet legislation but this becomes even more critical in a POPI environment. For starters we monitor email so that we can see what is going in and what's going out. There are certain triggers that if contained in that email it will send an alert, one of them is ID number for example so that we can see if ID numbers are leaving the organisation. Often sensitive data contains ID numbers so that's one way we look after our information. We also try to ensure that where sensitive information is communicated even with auditors or JV (Joint Venture) partners that we do it via secure file transfer protocol, set up SFTP site rather than just using normal FTP or email which is obviously not ideal. If files do have to be sent via email we'll ask that passwords are used and sent via a different channel to at least offer some mode of protection for those files. You'll find that devices as part of our IT policy are on lockdown and you are not able to use unauthorized USB's or flash drives. There's as I mentioned control over emails as well as when documents are printed there are certain triggers where managers will also be notified. These are all procedures that we put in place largely with a technological focus to protect our information. Then we also have house rules in place. Now currently as it stands house rules are not uniformly applied across the organisation. Departments have different house rules but the aim is to get us all to a place where we've got at least certain basics in place such as a clean desk policy, no cellphones in operational areas. It's one thing to be able to email information but we also vulnerable from a perspective where smart phones can take photographs. So these are all things we do to try to protect our information.

**8) Do you have policies in this institution dealing with information management? YES/NO**

Besides what we covered there's the bigger obvious one which is the physical access security policy so that we control access to not only the general precinct but also the more sensitive areas within the business that are access controlled like server rooms and so on. Otherwise it comes down pretty much to those rules and policies that I've mentioned.

**If YES, are they responsive or aligned to the national legislations?**

Up until this point they have largely been driven by what the organisation feels it needs because there haven't been specific legislation governing it. The closest thing that there is,

the operative sections of POPI have not yet come into effect. Portions of POPI have come in like the need to set up the regulator and the powers of the regulator. The operative section is really the one to govern the use of personal information is not yet in place. We obviously have a POPI project running and it's on our radar so we trying to take the appropriate steps so that when it does become available we will manage our data in a responsible fashion as a responsible party for data. It's not legislatively driven at the moment. There are also some internal controls where we try to run scans of our environment to see where information is sitting. For example another bit of information that is quite sensitive is credit information of our customers or our staff we've got to be careful that we not recording any credit card information and there's no need for anybody to be accumulating that type of information. We run scans on our environment from time to time. Whenever there is a presence of credit card data we also need to understand it better and any anomalies and address it. That credit card data is not part of legislation but there is something called Payment Card Industry (PCI) data security standards which actually applies more to credit card companies but because we are a member of banking there is certain expectations that we take the necessary steps to protect card data as well as in the merchant agreement that we have.

**What are the opportunities and challenges brought by this policy?**

It has to do with the way that we obtain information from customer and once we've got that information what we do with it. The thing about POPI is that you have to have the data for a specific purpose. There is a general clause that says if it's necessary for your commercial interest then it's justifiable to maintain this data however the concern there is that the commercial interest is going to be very narrowly defined and if we not going to be able to have the free for all on customer data that we had in the past. We'll have to look after data more carefully in the way that we share it, the way that it's shared with us and the way that we manage, for what purpose we use it and when we have to delete it. Even in the absence of POPI information is an asset, you do not need a law to tell you that you should be looking after information.

**If NO/YES, what are your organizational plans in place to ensure that your key stakeholders (employees and vendors etc.) do not breach information?**

The policies that are in place as discussed previously.

**What tools do you have in place to ensure that your key stakeholders do not breach information?**

You can either alert on information breaches or you block it completely. We know that a lot of our information goes out via email. The problem is a lot of them are related to valid business processes. If we were to block we would cause a serious bottleneck in business. We'd probably be responsible for bringing the business to a halt. We rather have an alert system. We have a program called websense, this triggers and notifies us of emails being sent out with certain data. It's then up to the managers, the managers get alerted, it is then up to them to take the necessary precautions. In terms of the preventative or locking down of the devices there's a way we control that. You can't bring you flash drive to work and put information it, you can't take the information off our systems.

## **SECTION C – INFORMATION MANAGEMENT MITIGATION IN A FINANCIAL INSTITUTION**

### **9) Do you have mitigation strategies on information management in this organization?**

**YES/NO**

Yes.

### **10) What are your mitigation plans in relation to information management?**

In terms of the strategy and the road map other than knowing that data is important and the steps of spoken through on technology and things we've done even ahead of the legislation to make sure we look after information as an asset. There is a central function called information governance and we have appointed someone looking after information is a major breakthrough in itself. There's work being done looking at what the group standards are in terms of information management and records management while doing a gap analysis on our standards. Also looking at what we do from an information perspective so that we do make progress on this journey.

### **11) Are staff members, other than executive management, aware and knowledgeable of the information management security policies put in place by the organisation? YES/NO**

I don't think they are as aware as they could be.

#### **a) If yes, what is done in order to achieve this?**

We are trying to increase awareness. Recently there have been campaigns running from an IT side like looking after passwords. There's also been awareness around POPI that was sent out. Quite recently there was communication sent to the business about key policies like social media policies, zero tolerance on non-compliance polices, IT systems acceptable user polices. These are our key foundational things that we

need to know. We've sent out teasers through our intranet in terms of what's coming. We've sent links to all of those policies. When staff log on to computers you have to acknowledge the regulations. More policies will be listed on this log on shortly, with a clear expectation that you know what these policies mean and you have to abide by them. If you don't know what they are get hold of your manager to figure it out because ignorance is not going to be an excuse to the regulator.

**b) If no, what does the organisation view as the being important in relation to information management?**

## **SECTION D – INFORMATION MANAGEMENT PREPAREDNESS IN A FINANCIAL INSTITUTION**

**12) Do you have preparedness plans to respond to any potential risk on information management? YES/NO**

Yes.

It depends on the seriousness of breach. Managers will get alerts and determine whether they are of a serious nature or if there's a valid explanation for it. When something comes up that is serious enough we will take it further. For example there was an issue with a scan that we ran whereby an individual had an unusual amount of PCI data and we actually landed up imaging that specific device. We called in specialists to analyse the origin of the data, what was done with it, etc. The person was suspended during the investigation. As it turned out there was nothing untoward there in that particular case but we viewed it seriously and we got experts in to help us so we deal with it on a case by case basis.

**a) How are government policies and regulations on information management aligned with this organisations policies?**

It's largely driven to what the organisation needs but we are preparing for the big information legislation policy of POPI which does not yet have the operative section in place by government.

**b) If it's not aligned, what are the organisations view on the future state to align this?**

## **SECTION E – INFORMATION MANAGEMENT SYSTEMS IN A FINANCIAL INSTITUTION**

### **13) How are the organisations technology systems aligned to the strategic plans of the organisation in relation to information management?**

I'm not really very well poised to answer that but at one stage there was a master data management program but I think that has now evolved into something else. There's also the data warehouse projects. It's gone through a couple of iterations I don't know quite where it is at the moment. There is a lot of different systems talking to each other also the single view of the customer that we trying to do. We've got information that is updated and overwritten at so many different levels.

#### **a) If it's not aligned, why?**

## **SECTION F – RISK RESPONSE AND RECOVERY IN A FINANCIAL INSTITUTION**

### **14) What are the organisations risk management plans to deal with information management breaches?**

Most of them have been covered in the previous sections. We could be better at it and we will need to get better at it when POPI comes in but there is the increased focus on information governance.



### Interview 3:

SUPERVISOR DETAILS	
Name:	Bethuel
Surname:	Ngcamu
Email:	Ngcamub@cput.ac.za

RESEARCH TITLE
An empirical investigation into the information management systems at a South African financial institution.
PURPOSE AND IMPACT OF STUDY
<p>The study has been triggered by the increase in information breaches in organisations. Organisations may have policies and procedures, strategies and systems in place in order to mitigate the risk of information breaches but the data breaches are still on the rise. Governments across the world have or are putting in place laws around data protection which organisations have to align their process, strategies and systems to.</p> <p>Organisational compliance on information is a topical issue that impacts many organisations. Many of these organisations have not fully come to grip with the actual implications to the business or understand how employees are dealing with this on a day to day basis. The research is important as it will assist a selected financial institution to fill a gap in the ability to handle information management in the organisation. As highlighted previously, there are many aspects of information which companies have to cater for such as government legislation and company policies as well as marrying these two up.</p>

HOW TO COMPLETE THE INTERVIEW AND THE TARGET POPULATION
<ul style="list-style-type: none"> <li>➤ This interview questions comprises of open-ended questions which requires the respondent to verbally respond to the questions.</li> <li>➤ The interview questions are aimed at executive management in the organisation.</li> <li>➤ The questions will be asked face to face by the researcher. If the question is not understood the researcher will be on hand to explain the question.</li> <li>➤ The researcher will document all answers to the questions represented on this interview question list.</li> </ul>

CONFIDENTIALITY AND ANONYMITY
Please note that ALL information provided by any respondent will be kept strictly confidential and the anonymity of the respondent is guaranteed.

SECTION A – BIOGRAPHICAL INFORMATION	
<b>1) Gender</b>	
Male	01X
Female	02
<b>2) Age</b>	
21-30	01
31-40	02X
41-50	03
51-60	04
60-65	05
65 and above	06
<b>3) Highest level of education completed</b>	
Below matric	01
Matric	02
Diploma	03
Bcom or Btech	04
Honours	05X
Masters	06
<b>4) What staffing level can you be classified in?</b>	
Executive Management	01
Senior Management (Non Executive)	02X
<b>5) What is your current job title?</b>	
Business Centre Leader: Value Added Products	
<b>6) How long have you been in this position at the company?</b>	
0 to 3 years	01
4 to 6 years	02X
7 to 10 years	03
More than 10 years	04

## SECTION B – BREACHING OF DATA IN A FINANCIAL INSTITUTION

### **7) What plans do you have to ensure that employees do not breach information in this organisation?**

There's a few initiatives in place. We've got a DPL breach that our IT departments manages so anything we pick up from an ID number or customer pertinent data that is sent externally via email or removed via a portable device. We have an internal process. I'm a key individual of the business as well so it's important that I practice what I preach. So specifically we have a clean desk policy. We've brought out standard operating procedures that agents or staff members in the business understands what the implications are for customer data to be breached and I think the team leaders have a daily process to make sure that they go through the desks after shifts to ensure that no customer information is left on desks because we have cleaning staff that come through in the evening as well as any documentation that you write down is kept in a secured environment like in a book in your draw, etc. Also none of our agents have external email. They are not allowed to have their smart phone devices on the operational floor.

### **8) Do you have policies in this institution dealing with information management? YES/NO** Yes.

#### **If YES, are they responsive or aligned to the national legislations?**

These polices discussed are generic for the company. We've got a standardised POPI (Protection of Personal Information Act), CPA (Consumer Protection Act) as well as our HR protocol all in place regarding data breaches. We also try to make sure that most of our partners transact via a SFTP (Secure File Transfer Protocol) to ensure that nobody is sending big pieces of data via email, it's all done on SFTP sites.

#### **What are the opportunities and challenges brought by this policy?**

It brings limitations for when you do need to use technology for real work. I think it takes away the empowerment of individuals that could have fulfilled a duty and now they can't because they don't have external email so I think it does add extra processes to operations and you may also find that it limits efficiency sometimes in certain business processes.

#### **If NO/YES, what are your organizational plans in place to ensure that your key stakeholders (employees and vendors etc.) do not breach information?**

I think that there is various checks. I always look at the DPL breaches as a key component of my role because all my senior manages DPL breaches comes to me so I actually follow up quite regularly to find out why was data sent out.

**What tools do you have in place to ensure that your key stakeholders do not breach information?**

I've actually put it in our, what we call our house rules policy. We have a house rules policy that everyone in our business is responsible for data protection so it's not just from top down. Everyone takes a serious approach to it but actual checks and balances is very reactive. Something must happen in order to go and see if there's enough processes in place to mitigate it. I don't think we'll ever eradicate it I think it's a mitigation strategy.

**SECTION C – INFORMATION MANAGEMENT MITIGATION IN A FINANCIAL INSTITUTION**

**9) Do you have in this organization mitigation strategies on information management?**

**YES/NO**

Yes.

**10) What are your mitigation plans in relation to information management?**

I think there's a lot of structure at the company. We've got a Data Governance Council (DGC) that was recently formed. For the first time I think we bringing the right people in the room to talk about data and data restrictions. Just by bringing about a data governance structure as in what ifs and what not to do's is the first stance. We take for granted that data is also good for what we do as a business but it can also be to our demise if something goes wrong so I think overall strategy is that we finally have an owner for data governance. It's filtered down through to data stewards throughout the business. From the data stewards it's then managed within the different silos with specific governance structures and I think they've drafted memorandum of understanding so everybody understands what the council is there for. It's not there to be a bottleneck for the business but definitely mitigate risk going forward and this council meets on a monthly basis to understand what the breaches of this company has been how have we mitigated it. Simple things would be a laptop goes missing with specific data on it and the how do we approach it. I definitely think the strategy is for the first time we've actually got a structure for data governance.

**11) Are staff members, other than executive management, aware and knowledgeable of the information management security policies put in place by the organisation? YES/NO**

Yes.

**a) If yes, what is done in order to achieve this?**

They've formally launched the Data Governance Council about four months ago and it's got quite a lot of senior attendees so head of risk, head of marketing, the collections strategy is in there so the good thing it's been played down to sort of junior levels as well on the importance of the council.

**b) If no, what does the organisation view as the being important in relation to information management?**

**SECTION D – INFORMATION MANAGEMENT PREPAREDNESS IN A FINANCIAL INSTITUTION**

**12) Do you have preparedness plans to respond to any potential risk on information management? YES/NO**

I think we quite scripted in the sense, or more process orientated in the sense data breaches were always regarded as a customer originated risk. It needs to be both, if we know that we breached customer data we need to obviously go out in public domain and mention it. I think the uncertainty is that we work within a call centre environment and people are becoming more familiar with what their rights are. When we speak to customers telephony wise, when a customer says where did you get my information from? We must be very clear and provide them with it. There's a lot of company's out there and I've done this myself and I've asked sales people on the telephone where did you get my information from? And the phone goes dead. This company must just be scripted, what I mean in the word scripted I think we've scripted ourselves where we can say you've opted in on this day that time on this channel, you've said it's a marketing consent for a specific product and the verse of that would be that if a customer says to me do not ever call me again do not promote we take that record and we keep it and we make sure that we don't do that in the future. It's not just about housing the data but I think it's also about making sure that verbatim we can tell customers when we received your marketing consent, why and if we look at if there's a breach in a sense that a website opens up, there's been a few articles in the last 3 months that the equivalent of Woolies in the UK, MNS. When customers went onto a website and they could actually see other customer's information. We want to make sure that we manage that from a communication aspect. I think we've got that pegged down that we not going to lie to customers we quite open because our brand is about being that.

**a) How are government policies and regulations on information management aligned with this organisations policies?**

You've got Treat Customer Fairly, there's POPI, there's CPA, there's the DMA (Direct Marketing Association), there's this company's group governance structure.

**b) If it's not aligned, what are the organisations view on the future state to align this?**

**SECTION E – INFORMATION MANAGEMENT SYSTEMS IN A FINANCIAL INSTITUTION**

**13) How are the organisations technology systems aligned to the strategic plans of the organisation in relation to information management?**

We purely talking to it from a data governance structure I think every user is set up in this business to have certain administrator rights, some have more, some have less based on the role. A very simple example I would use in my role our strategy is to sell value added products on the back of a loan agreement. If you think of customers in the loans space they give you specific banking details to pay a loan in. So what we have done on our side we've decided to omit that information to our agents when they do cross selling because the risk of them just adding customer banking details to a product without actually speaking to a customer is too high. We've eradicated that as a risk area a while ago. We've said when we offer data for lead segmentation rules or positioning, we actually omit banking information as a prerequisite.

**b) If it's not aligned, why?**

**SECTION F – RISK RESPONSE AND RECOVERY IN A FINANCIAL INSTITUTION**

**14) What are the organisations risk management plans to deal with information management breaches?**

I think the communication is that we have got nothing to hide, we quite clear and open. If we ever breach a data risk but with structure coming into place now with the DGC I definitely foresee more focus on when we have breached. The example would be most of our business is telephony driven so a lot of our calls are stored offsite and onsite and I've definitely seen a clean up to make sure that the agreements with these vendors externally and internally are much more specific so that we can assure ourselves, it's not just about hard data, it's about voice recordings, where they stored, how they stored, what is the retrieval process of these calls so I think there's more focus on making sure that our third party vendors and partners that we use for structures to ether safe keep or store are in place prior to what it was before.

#### Interview 4:

SUPERVISOR DETAILS	
Name:	Bethuel
Surname:	Ngcamu
Email:	Ngcamub@cput.ac.za

RESEARCH TITLE
An empirical investigation into the information management systems at a South African financial institution.
PURPOSE AND IMPACT OF STUDY
<p>The study has been triggered by the increase in information breaches in organisations. Organisations may have policies and procedures, strategies and systems in place in order to mitigate the risk of information breaches but the data breaches are still on the rise. Governments across the world have or are putting in place laws around data protection which organisations have to align their process, strategies and systems to.</p> <p>Organisational compliance on information is a topical issue that impacts many organisations. Many of these organisations have not fully come to grip with the actual implications to the business or understand how employees are dealing with this on a day to day basis. The research is important as it will assist a selected financial institution to fill a gap in the ability to handle information management in the organisation. As highlighted previously, there are many aspects of information which companies have to cater for such as government legislation and company policies as well as marrying these two up.</p>

HOW TO COMPLETE THE INTERVIEW AND THE TARGET POPULATION
<ul style="list-style-type: none"> <li>➤ This interview questions comprises of open-ended questions which requires the respondent to verbally respond to the questions.</li> <li>➤ The interview questions are aimed at executive management in the organisation.</li> <li>➤ The questions will be asked face to face by the researcher. If the question is not understood the researcher will be on hand to explain the question.</li> <li>➤ The researcher will document all answers to the questions represented on this interview question list.</li> </ul>

CONFIDENTIALITY AND ANONYMITY
Please note that ALL information provided by any respondent will be kept strictly confidential and the anonymity of the respondent is guaranteed.

SECTION A – BIOGRAPHICAL INFORMATION	
<b>1) Gender</b>	
Male	01X
Female	02
<b>2) Age</b>	
21-30	01
31-40	02
41-50	03
51-60	04X
60-65	05
65 and above	06
<b>3) Highest level of education completed</b>	
Below matric	01
Matric	02
Diploma	03
Bcom or Btech	04X
Honours	05
Masters	06
<b>4) What staffing level can you be classified in?</b>	
Executive Management	01
Senior Management (Non Executive)	02X
<b>5) What is your current job title?</b>	
Business Centre Leader: IT Operations	
<b>6) How long have you been in this position at the company?</b>	
0 to 3 years	01X
4 to 6 years	02
7 to 10 years	03
More than 10 years	04

## **SECTION B – BREACHING OF DATA IN A FINANCIAL INSTITUTION**

**7) What plans do you have to ensure that employees do not breach information in this organisation?**

The IT security policy governs that, in terms of what access people have and what access to what systems they have.

**8) Do you have policies in this institution dealing with information management? YES/NO**

Yes.

**If YES, are they responsive or aligned to the national legislations?**

Because we a financial institution we have to be compliant in terms of anything that's legislative from a regulatory perspective for the industry and from a compliance perspective also from an internal governance perspective.

**What are the opportunities and challenges brought by this policy?**

There are lots of challenges for us as a financial institution. As we retain customer data we sometimes can't make use of the latest trends or technologies that can help us to improve the business or to save money.

**If NO/YES, what are your organizational plans in place to ensure that your key stakeholders (employees and vendors etc.) do not breach information?**

We have policies in place that all employees are made aware of and we have contracts in place with our vendors.

**What tools do you have in place to ensure that your key stakeholders do not breach information?**

We have a couple of security tools. We've got a tool that blocks the use of USB devices, we've got a device that alerts you when people copy or forward confidential information.

## **SECTION C – INFORMATION MANAGEMENT MITIGATION IN A FINANCIAL INSTITUTION**

**9) Do you have in this organization mitigation strategies on information management? YES/NO**

Yes, there are.

**10) What are your mitigation plans in relation to information management?**

We do things like penetration testing to see how secure our data is from the outside. We do internal penetration to make sure how easily accessible it is for people to access the systems or change passwords. We also have a security event and incident management system.

**11) Are staff members, other than executive management, aware and knowledgeable of the information management security policies put in place by the organization? YES/NO**

Yes.

**a) If yes, what is done in order to achieve this?**

We have a communication strategy so we try and run two awareness campaigns on information security per year.

**b) If no, what does the organisation view as the being important in relation to information management?**

**SECTION D – INFORMATION MANAGEMENT PREPAREDNESS IN A FINANCIAL INSTITUTION**

**12) Do you have preparedness plans to respond to any potential risk on information management? YES/NO**

Yes.

**a) How are government policies and regulations on information management aligned with this organisations policies?**

The IT audit governs us in terms, we do internal and external auditing that governs the plans we put in place to ensure if there are any gaps that we close those gaps. The audit is based on best practice in terms of IT standards and also legislative from a group perspective to ensure that information is secure.

**b) If it's not aligned, what are the organisations view on the future state to align this?**

**SECTION E – INFORMATION MANAGEMENT SYSTEMS IN A FINANCIAL INSTITUTION**

**13) How are the organisations technology systems aligned to the strategic plans of the organisation in relation to information management?**

We a bit behind the times but we've got projects on the go at the moment around identity and access management. This is so that we have one system that controls access to information and also governs the people that have access to information.



a) If it's not aligned, why?

**SECTION F – RISK RESPONSE AND RECOVERY IN A FINANCIAL INSTITUTION**

**14) What are the organisations risk management plans to deal with information management breaches?**

We've done some forensic training to make sure that if we ever have a breach that we are able to secure the data we would need for the forensic investigation and also we have alerting in place for when people try to delete data or access data in terms of unauthorised access to data which will notify their manager.

## Interview 5:

SUPERVISOR DETAILS	
Name:	Bethuel
Surname:	Ngcamu
Email:	Ngcamub@cput.ac.za

RESEARCH TITLE
An empirical investigation into the information management systems at a South African financial institution.
PURPOSE AND IMPACT OF STUDY
<p>The study has been triggered by the increase in information breaches in organisations. Organisations may have policies and procedures, strategies and systems in place in order to mitigate the risk of information breaches but the data breaches are still on the rise. Governments across the world have or are putting in place laws around data protection which organisations have to align their process, strategies and systems to.</p> <p>Organisational compliance on information is a topical issue that impacts many organisations. Many of these organisations have not fully come to grip with the actual implications to the business or understand how employees are dealing with this on a day to day basis. The research is important as it will assist a selected financial institution to fill a gap in the ability to handle information management in the organisation. As highlighted previously, there are many aspects of information which companies have to cater for such as government legislation and company policies as well as marrying these two up.</p>

HOW TO COMPLETE THE INTERVIEW AND THE TARGET POPULATION
<ul style="list-style-type: none"> <li>➤ This interview questions comprises of open-ended questions which requires the respondent to verbally respond to the questions.</li> <li>➤ The interview questions are aimed at executive management in the organisation.</li> <li>➤ The questions will be asked face to face by the researcher. If the question is not understood the researcher will be on hand to explain the question.</li> <li>➤ The researcher will document all answers to the questions represented on this interview question list.</li> </ul>

CONFIDENTIALITY AND ANONYMITY
Please note that ALL information provided by any respondent will be kept strictly confidential and the anonymity of the respondent is guaranteed.

SECTION A – BIOGRAPHICAL INFORMATION	
<b>1) Gender</b>	
Male	01X
Female	02
<b>2) Age</b>	
21-30	01
31-40	02
41-50	03
51-60	04X
60-65	05
65 and above	06
<b>3) Highest level of education completed</b>	
Below matric	01
Matric	02
Diploma	03
Bcom or Btech	04
Honours	05
Masters	06X
<b>4) What staffing level can you be classified in?</b>	
Executive Management	01X
Senior Management (Non Executive)	02
<b>5) What is your current job title?</b>	
Head of IT	
<b>6) How long have you been in this position at the company?</b>	
0 to 3 years	01X
4 to 6 years	02
7 to 10 years	03
More than 10 years	04

## SECTION B – BREACHING OF DATA IN A FINANCIAL INSTITUTION

**7) What plans do you have to ensure that employees do not breach information in this organisation?**

Technologically we have disabled all external devices on PC's which means that they can't copy any data directly. On email we've got email security. The third one is penetration tests and vulnerability assessments on a regular basis both internally and externally.

**8) Do you have policies in this institution dealing with information management? YES/NO**

Yes, we have the standard policies.

**If YES, are they responsive or aligned to the national legislations?**

The policies are aligned to national and industry standards.

**What are the opportunities and challenges brought by this policy?**

The biggest challenge is it reduces flexibility and creativity. There is a bit of limitations and that's obviously the negative. The opportunity is that there is a clear guideline and standard that everybody is aware of and complies with. Our compliance requirement is fairly well met.

**If NO/YES, what are your organizational plans in place to ensure that your key stakeholders (employees and vendors etc.) do not breach information?**

I've answered that question already around hardware devices.

**What tools do you have in place to ensure that your key stakeholders do not breach information?**

[RA] The interviewee has answered this in a previous answer noting to hardware devices.

## SECTION C – INFORMATION MANAGEMENT MITIGATION IN A FINANCIAL INSTITUTION

**9) Do you have, in this organization, mitigation strategies on information management? YES/NO**

There's the HR disciplinary process, if and when someone does not comply. We also have firewall technology to protect what comes in and goes out and then obviously we've got virus management which is the third one.

**10) What are your mitigation plans in relation to information management?**

[RA] The interviewee had already referred to firewall technology and virus management.

**11) Are staff members, other than executive management, aware and knowledgeable of the information management security policies put in place by the organization? YES/NO**

Yes.

**a) If yes, what is done in order to achieve this?**

We do run a full awareness program of the security policy as well as continuously updating the current policies to make it relevant to the current times.

**b) If no, what does the organisation view as the being important in relation to information management?**

#### **SECTION D – INFORMATION MANAGEMENT PREPAREDNESS IN A FINANCIAL INSTITUTION**

**12) Do you have preparedness plans to respond to any potential risk on information management? YES/NO**

We have a breach management policy and practice in place. We have crisis management. Breach management is part of the crisis management process.

**a) How are government policies and regulations on information management aligned with this organisations policies?**

Yes it's aligned.

**b) If it's not aligned, what are the organisations view on the future state to align this?**

#### **SECTION E – INFORMATION MANAGEMENT SYSTEMS IN A FINANCIAL INSTITUTION**

**13) How are the organisations technology systems aligned to the strategic plans of the organisation in relation to information management?**

We fully aligned, well let's say there is alignment between the business strategy and information management.

**a) If it's not aligned, why?**

#### **SECTION F – RISK RESPONSE AND RECOVERY IN A FINANCIAL INSTITUTION**

**14) What are the organisations risk management plans to deal with information management breaches?**

It speaks to preparedness plans.

## Interview 6:

SUPERVISOR DETAILS	
Name:	Bethuel
Surname:	Ngcamu
Email:	Ngcamub@cput.ac.za

RESEARCH TITLE
An empirical investigation into the information management systems at a South African financial institution.
PURPOSE AND IMPACT OF STUDY
<p>The study has been triggered by the increase in information breaches in organisations. Organisations may have policies and procedures, strategies and systems in place in order to mitigate the risk of information breaches but the data breaches are still on the rise. Governments across the world have or are putting in place laws around data protection which organisations have to align their process, strategies and systems to.</p> <p>Organisational compliance on information is a topical issue that impacts many organisations. Many of these organisations have not fully come to grip with the actual implications to the business or understand how employees are dealing with this on a day to day basis. The research is important as it will assist a selected financial institution to fill a gap in the ability to handle information management in the organisation. As highlighted previously, there are many aspects of information which companies have to cater for such as government legislation and company policies as well as marrying these two up.</p>

HOW TO COMPLETE THE INTERVIEW AND THE TARGET POPULATION
<ul style="list-style-type: none"> <li>➤ This interview questions comprises of open-ended questions which requires the respondent to verbally respond to the questions.</li> <li>➤ The interview questions are aimed at executive management in the organisation.</li> <li>➤ The questions will be asked face to face by the researcher. If the question is not understood the researcher will be on hand to explain the question.</li> <li>➤ The researcher will document all answers to the questions represented on this interview question list.</li> </ul>

CONFIDENTIALITY AND ANONYMITY
Please note that ALL information provided by any respondent will be kept strictly confidential and the anonymity of the respondent is guaranteed.

SECTION A – BIOGRAPHICAL INFORMATION	
<b>1) Gender</b>	
Male	01
Female	02X
<b>2) Age</b>	
21-30	01
31-40	02
41-50	03
51-60	04X
60-65	05
65 and above	06
<b>3) Highest level of education completed</b>	
Below matric	01
Matric	02
Diploma	03
Bcom or Btech	04
Honours	05
Masters	06X
<b>4) What staffing level can you be classified in?</b>	
Executive Management	01X
Senior Management (Non Executive)	02
<b>5) What is your current job title?</b>	
Head of People	
<b>6) How long have you been in this position at the company?</b>	
0 to 3 years	01
4 to 6 years	02
7 to 10 years	03X
More than 10 years	04

## SECTION B – BREACHING OF DATA IN A FINANCIAL INSTITUTION

### 7) What plans do you have to ensure that employees do not breach information in this organisation?

Firstly from a policy perspective we've got a number of policies that informs staff about what is a breach and what's not a breach. The second thing that we have is through induction process people get informed on what is a breach and what's not a breach. Thirdly from a quality assurance perspective when quality assessors listen to calls they know when information is being breached or not and in HR what I've done is I put in first level of control, second level of control so that when somebody is working with something and they not sure then someone is checking it so there is enough division of labour and division of duties. Segregation of duties is what we put in place and I think also from a breach of confidentiality it's just when you recruit people from an HR perspective I make sure that my team knows the information they deal with is confidential and if they break confidentiality I take disciplinary action. On a simple level if we sending out salary information or pay slips it's always password protected.

### 8) Do you have policies in this institution dealing with information management? YES/NO

Yes.

**If YES, are they responsive or aligned to the national legislations?**

Yes.

**What are the opportunities and challenges brought by this policy?**

From a challenge point of view I think it's just to keep it top of mind for people. How to keep reminding people and we use e-learning modules that people have to keep doing modules every year to remind them. We deal with a lot of staff information so one of my challenges is storage on information. We keep it online, we also keep it in a secure filing space down stairs so I think our challenges are just making sure that people abide by the policies. I think the opportunity are around reinforcing privacy, getting ready for legislation like POPI (Protection of Personal Information Act) and just giving staff the assurance. For example administer a lot of salary information, we administer people apply for loans, staff applies for advances and it stays very confidential. If we were blabbing about the things we do nobody would trust us.

**If NO/YES, what are your organizational plans in place to ensure that your key stakeholders (employees and vendors etc.) do not breach information?**

[RA] the interviewee has mentioned this in the previous answer. I.e. keeping information online and in a secure filing space and e-learning modules to educate stakeholders.

**What tools do you have in place to ensure that your key stakeholders do not breach information?**

I mentioned password protections, e-learning modules. From an IT perspective there's a warning that goes when someone is emailing anything with staff numbers on it or with ID numbers on it. That gets flagged and sent to me because sometimes my team works at home and they don't take their laptops so they email stuff home but I immediately know when there's a security breach because the alerts come back to me so we've got alerts built into an IT system. What I will do is investigate that. The moment I get an alert I phone the person and ask what is it? So they know, my team won't take a chance or what they'll do they tell me in advance that we about to do this.

**SECTION C – INFORMATION MANAGEMENT MITIGATION IN A FINANCIAL INSTITUTION**

**9) Do you have, in this organization, mitigation strategies on information management?**

**YES/NO**

Yes.

**10) What are your mitigation plans in relation to information management?**

This covered in the alerts. Proactively in terms of the password protection and the fact that information is locked away. What we've also done is from payroll perspective we've separated out executive payroll and put it into an outside company so we've outsourced executive payroll. Only the MD (Managing Director) has access to that information and can release the payments.

**11) Are staff members, other than executive management, aware and knowledgeable of the information management security policies put in place by the organisation? YES/NO**

Yes.

**a) If yes, what is done in order to achieve this?**

[RA] The interviewee answered this in a previous question. I.e. E-learning modules to educate employees and in the induction process people are informed.

**b) If no, what does the organisation view as the being important in relation to information management?**

## SECTION D – INFORMATION MANAGEMENT PREPAREDNESS IN A FINANCIAL INSTITUTION

### **12) Do you have preparedness plans to respond to any potential risk on information management? YES/NO**

Yes. We use our normal disciplinary process. If anything is breached we will use our normal IR (Industrial Relations) process. The other part of preparedness is at induction stage when you come to work for HR you know about confidentiality, about looking after information and not sharing information.

### **a) How are government policies and regulations on information management aligned with this organisations policies?**

Focusing specifically on confidentiality there is no requirement on confidentiality I think it's just a code of ethics for anybody who works in HR to know you can't share information.

### **b) If it's not aligned, what are the organisations view on the future state to align this?**

## SECTION E – INFORMATION MANAGEMENT SYSTEMS IN A FINANCIAL INSTITUTION

### **13) How are the organisations technology systems aligned to the strategic plans of the organisation in relation to information management?**

From a HR software system perspective the granting of access is held centrally and is given to a line manager and that line manager can only see their people's information. They can't see everybody else's information. There is a workflow and an IT perspective. There is password protection in anything we do, whether it's VIP pay slips everything is password protected. We've kept our payroll system separate from our admin system. Three people have access to the payroll system. Even in finance when we paying invoices to third parties sometimes salaries get billed for a person you placing and their salary information is on there because it's 10% or 15% of what the person earns so we can work it out. When it comes to HR we have the person's name on it, we then sign the form and we blank it out, we keep two copies, one is with the persons actual name on it, we submit the blank to finance. It's a very manual process but that's what we do.

### **b) If it's not aligned, why?**



**14) What are the organisations risk management plans to deal with information management breaches?**

We take disciplinary action. Secondly from an IT perspective we've built in early warning signals for the signals that tells us when information is being breached. Thirdly we will notify, so if a customer's information is breached I think we would notify the customer. I know that that if there's a big scale of fraud going down we will notify our shareholders so we'll manage shareholder expectation and I think anything we can do to minimise reputational damage. If customers thought that suddenly information that they give us, like they give is salary information because of affordability we have to protect all of that. I think with call centre staff we discourage them from writing so capture everything online, capture everything on the system, don't write ID numbers down and then in the evening when cleaners walk around they are trained to look for those things and if they see it they destroy it. We've also got safety bins, secured bins to get rid of papers.

## Interview 7:

SUPERVISOR DETAILS	
Name:	Bethuel
Surname:	Ngcamu
Email:	Ngcamub@cput.ac.za

RESEARCH TITLE
An empirical investigation into the information management systems at a South African financial institution.
PURPOSE AND IMPACT OF STUDY
<p>The study has been triggered by the increase in information breaches in organisations. Organisations may have policies and procedures, strategies and systems in place in order to mitigate the risk of information breaches but the data breaches are still on the rise. Governments across the world have or are putting in place laws around data protection which organisations have to align their process, strategies and systems to.</p> <p>Organisational compliance on information is a topical issue that impacts many organisations. Many of these organisations have not fully come to grip with the actual implications to the business or understand how employees are dealing with this on a day to day basis. The research is important as it will assist a selected financial institution to fill a gap in the ability to handle information management in the organisation. As highlighted previously, there are many aspects of information which companies have to cater for such as government legislation and company policies as well as marrying these two up.</p>

HOW TO COMPLETE THE INTERVIEW AND THE TARGET POPULATION
<ul style="list-style-type: none"> <li>➤ This interview questions comprises of open-ended questions which requires the respondent to verbally respond to the questions.</li> <li>➤ The interview questions are aimed at executive management in the organisation.</li> <li>➤ The questions will be asked face to face by the researcher. If the question is not understood the researcher will be on hand to explain the question.</li> <li>➤ The researcher will document all answers to the questions represented on this interview question list.</li> </ul>

CONFIDENTIALITY AND ANONYMITY
Please note that ALL information provided by any respondent will be kept strictly confidential and the anonymity of the respondent is guaranteed.

SECTION A – BIOGRAPHICAL INFORMATION	
<b>1) Gender</b>	
Male	01X
Female	02
<b>2) Age</b>	
21-30	01
31-40	02X
41-50	03
51-60	04
60-65	05
65 and above	06
<b>3) Highest level of education completed</b>	
Below matric	01
Matric	02X
Diploma	03
Bcom or Btech	04
Honours	05
Masters	06
<b>4) What staffing level can you be classified in?</b>	
Executive Management	01
Senior Management (Non Executive)	02X
<b>5) What is your current job title?</b>	
Business Centre Leader: Decision Technologies	
<b>6) How long have you been in this position at the company?</b>	
0 to 3 years	01X
4 to 6 years	02
7 to 10 years	03
More than 10 years	04

## SECTION B – BREACHING OF DATA IN A FINANCIAL INSTITUTION

**7) What plans do you have to ensure that employees do not breach information in this organisation?**

I follow the organization security controls which currently is run on certain data that when breach notification is sent to me. I however have no visibility of what those controls and measures are.

**8) Do you have policies in this institution dealing with information management? YES/NO**

No. We do in the decisioning risk space we have a document that is user controlled. It's access management only.

**If YES, are they responsive or aligned to the national legislations?**

**What are the opportunities and challenges brought by this policy?**

**If NO/YES, what are your organizational plans in place to ensure that your key stakeholders (employees and vendors etc.) do not breach information?**

**What tools do you have in place to ensure that your key stakeholders do not breach information?**

## SECTION C – INFORMATION MANAGEMENT MITIGATION IN A FINANCIAL INSTITUTION

**9) Does the organisation have mitigation strategies on information management? YES/NO**

No, not in my area.

The technologies we work on will but we don't have any mitigating circumstances. Any user scan screenshot any data any time. USB ports are blocked for any memory device downloads however emailed is uncontrolled, laptops aren't encrypted.

**10) What are your mitigation plans in relation to information management?**

The technologies we work on will but we don't have any mitigating circumstances. Any user scan screenshot any data any time. USB ports are blocked for any memory device downloads however emailed is uncontrolled, laptops aren't encrypted.

**11) Are staff members, other than executive management, aware and knowledgeable of the information management security policies put in place by the organisation? YES/NO**

No, absolutely not. I'm pretty sure it's documented somewhere but I haven't even seen it.

**a) If yes, what is done in order to achieve this?**

**b) If no, what does the organisation view as the being important in relation to information management?**

I think the organisation takes its serious however they lack in execution. I think we can change a lot more, be more cautious and conscious of our information security.

#### **SECTION D – INFORMATION MANAGEMENT PREPAREDNESS IN A FINANCIAL INSTITUTION**

**12) Do you have preparedness plans to respond to any potential risk on information management? YES/NO**

None that I am aware of.

**a) How are government policies and regulations on information management aligned with this organisations policies?**

So if we use POPI (Protection of Personal Information Act) as an example we are definitely regulated. With our joint venture partners we are definitely regulated with data sharing and data privacy. Again, execution and management and controls are lacking.

**b) If it's not aligned, what are the organisations view on the future state to align this?**

#### **SECTION E – INFORMATION MANAGEMENT SYSTEMS IN A FINANCIAL INSTITUTION**

**13) How are the organisations technology systems aligned to the strategic plans of the organisation in relation to information management?**

I don't believe they currently aligned but they are being adjusted to become aligned so again if we use POPI as an example impact assessments are being done on the regulatory changes where IT systems will be impacted and how they are impacted and what changes need to be made. Currently I would say we probable about 40% compliant. We've got a long way to go still. We've got business processes and rules in place like no cellphone on the floor but it's not managed or controlled.

**a) If it's not aligned, why?**

I think it's the execution of it. So again as per previous question we take it seriously but we lacking in the execution and control of it.

## **SECTION G – RISK RESPONSE AND RECOVERY IN A FINANCIAL INSTITUTION**

### **14) What are the organisations risk management plans to deal with information management breaches?**

No clue, again I'm sure it's documented somewhere.

## Interview 8:

SUPERVISOR DETAILS	
Name:	Bethuel
Surname:	Ngcamu
Email:	Ngcamub@cput.ac.za

RESEARCH TITLE
An empirical investigation into the information management systems at a South African financial institution.
PURPOSE AND IMPACT OF STUDY
<p>The study has been triggered by the increase in information breaches in organisations. Organisations may have policies and procedures, strategies and systems in place in order to mitigate the risk of information breaches but the data breaches are still on the rise. Governments across the world have or are putting in place laws around data protection which organisations have to align their process, strategies and systems to.</p> <p>Organisational compliance on information is a topical issue that impacts many organisations. Many of these organisations have not fully come to grip with the actual implications to the business or understand how employees are dealing with this on a day to day basis. The research is important as it will assist a selected financial institution to fill a gap in the ability to handle information management in the organisation. As highlighted previously, there are many aspects of information which companies have to cater for such as government legislation and company policies as well as marrying these two up.</p>

HOW TO COMPLETE THE INTERVIEW AND THE TARGET POPULATION
<ul style="list-style-type: none"> <li>➤ This interview questions comprises of open-ended questions which requires the respondent to verbally respond to the questions.</li> <li>➤ The interview questions are aimed at executive management in the organisation.</li> <li>➤ The questions will be asked face to face by the researcher. If the question is not understood the researcher will be on hand to explain the question.</li> <li>➤ The researcher will document all answers to the questions represented on this interview question list.</li> </ul>

CONFIDENTIALITY AND ANONYMITY
Please note that ALL information provided by any respondent will be kept strictly confidential and the anonymity of the respondent is guaranteed.

SECTION A – BIOGRAPHICAL INFORMATION	
<b>1) Gender</b>	
Male	01X
Female	02
<b>2) Age</b>	
21-30	01
31-40	02
41-50	03X
51-60	04
60-65	05
65 and above	06
<b>3) Highest level of education completed</b>	
Below matric	01
Matric	02
Diploma	03
Bcom or Btech	04
Honours	05X
Masters	06
<b>4) What staffing level can you be classified in?</b>	
Executive Management	01
Senior Management (Non Executive)	02X
<b>5) What is your current job title?</b>	
Business Centre Leader: Enterprise Architecture	
<b>6) How long have you been in this position at the company?</b>	
0 to 3 years	01X
4 to 6 years	02
7 to 10 years	03
More than 10 years	04

## SECTION B – BREACHING OF DATA IN A FINANCIAL INSTITUTION

### **7) What plans do you have to ensure that employees do not breach information in this organisation?**

The security architecture is my responsibility so the reality is that we have a plan for breaches. The execution happens in operations, so someone in IT will indirectly inform me or I'll influence him in terms of what is he doing around this. We going to be putting in new systems, policies, procedures, monitoring around understanding across the board, both users and the back end into servers, what they using, when they using it, how they using it and trying to also come up with system breaches. The reality of the fact is that we not there, we have a long way to go but we started the process to mature ourselves in that context.

### **8) Do you have policies in this institution dealing with information management? YES/NO**

There's two parts of information management. I'm talking about information management in general, Eric's team. In that case I'm not directly responsible but I am aware because I'm working with the Data Governance Council known as the DGC has to ensure that there's policies and procedures. Still, there's probably gaps but the council has to ensure that all those policies and procedures are in place. It's a work in progress.

#### **What are the opportunities and challenges brought by this policy?**

[RA] In the previous question the interviewee said that the Data Governance Council is responsible putting policies in place and that it's still a work in progress therefore I did not ask this question.

#### **If NO/YES, what are your organizational plans in place to ensure that your key stakeholders (employees and vendors etc.) do not breach information?**

[RA] In a previous question the interviewee said that the Data Governance Council is responsible putting policies in place and that it's still a work in progress therefore I did not ask this question.

#### **What tools do you have in place to ensure that your key stakeholders do not breach information?**

[RA] In a previous question the interviewee said that the Data Governance Council is responsible putting policies in place and that it's still a work in progress therefore I did not ask this question.

**SECTION C – INFORMATION MANAGEMENT MITIGATION IN A FINANCIAL INSTITUTION**

**9) Do you have, in this organization, mitigation strategies on information management?**

**YES/NO**

There are plans.

**10) What are your mitigation plans in relation to information management?**

Our strategy is around the fact that we don't have a view of information or consistent view of information. It's fragmented and to a certain extent results in the wrong decisions, etc. So the strategy is to put in systems and processes to manage that and really focus primarily around customer. We currently busy with a project doing a proof of concept to put in a Master Data Management (MDM) tool. We see master data like customer data, like reference data, etc. being very sporadic and different across the company so really the strategy is to fix that. Hopefully we'll start a project to actually implement something early next year. Another part is we also have an issue of other operational data and one of things I saw there wasn't a common business dictionary. BI (Business Intelligence) becomes a challenge. A field is called something in one place and something else in another place and then how do we tie them together so one of the things we doing in that MDM space is we going to be creating a common business vocabulary around information.

**11) Are staff members, other than executive management, aware and knowledgeable of the information management security policies put in place by the organisation? YES/NO**

Yes. It's probably not across the whole company but those who are involved.

**a) If yes, what is done in order to achieve this?**

If I use the information management side around MDM and the DGC and the policies and procedures as well. The developers from an IT perspective, the BI team, and the architects are aware of this. Most of the guys are involved in actually helping us define this and build this.

**b) If no, what does the organisation view as the being important in relation to information management?**

**SECTION D – INFORMATION MANAGEMENT PREPAREDNESS IN A FINANCIAL INSTITUTION**

**12) Do you have preparedness plans to respond to any potential risk on information management? YES/NO**



No, something that will have to go on the to-do list.

**a) How are government policies and regulations on information management aligned with this organisations policies?**

Regulation is key. Definitely it's applicable with POPI (Protection of Personal Information Act) coming our way. Our systems will have to be compliant and will have to be able to execute on all the regulatory requirements around compliance from an information management perspective. What we doing right now, we not fully ready on those new things like Radar and POPI but projects have started to actually understand the impact and to come up with sort of a solution.

**b) If it's not aligned, what are the organisations view on the future state to align this?**

[RA] In the previous question the interviewee stated that projects are under way to come up with a solution.

**SECTION E – INFORMATION MANAGEMENT SYSTEMS IN A FINANCIAL INSTITUTION**

**13) How are the organisations technology systems aligned to the strategic plans of the organisation in relation to information management?**

Our current systems are not aligned on information integration. Some systems doesn't integrate with other systems at all. The strategy is the 100% product offer. It can't be done in our current systems from an information management perspective, well it can be done but then it's done manually and ineffectively, it's not optimal and there's a high risk of error. For the future target architecture, we are busy putting together what it will look like and this will have to address these things. The target architecture is modelled on the business strategy. A key part in the business strategy is right time experience and this requires extensive information and analytics management.

**a) If it's not aligned, why?**

[RA] In the previous question the interviewee noted that the target architecture is being modelled to the business strategy.

**SECTION F – RISK RESPONSE AND RECOVERY IN A FINANCIAL INSTITUTION**

**14) What are the organisations risk management plans to deal with information management breaches?**

We actually had an incident not too long ago where call recording got removed and that enabled us to put a whole lot of policies and procedures in place and enabled us to actually understand how we actually go about investigating breaches and what the process is. We did a forensic audit on that. From a preparedness perspective the fact that we had to do it before we now understand the processes and lessons learnt from how to get continuous improvement. The challenge is that sometimes we are reactive instead of proactive. How we get to pro-activeness is going to take a long time. I think there is preparedness to react, preparedness to execute on an investigation or on a recovery but maybe sometimes we only find out after the fact and maybe sometimes we don't even know and that's reality. We don't have all the monitors, all the tools and all the ways of picking up breaches or loss of data as well.

## Interview 9:

SUPERVISOR DETAILS	
Name:	Bethuel
Surname:	Ngcamu
Email:	Ngcamub@cput.ac.za

RESEARCH TITLE
An empirical investigation into the information management systems at a South African financial institution.
PURPOSE AND IMPACT OF STUDY
<p>The study has been triggered by the increase in information breaches in organisations. Organisations may have policies and procedures, strategies and systems in place in order to mitigate the risk of information breaches but the data breaches are still on the rise. Governments across the world have or are putting in place laws around data protection which organisations have to align their process, strategies and systems to.</p> <p>Organisational compliance on information is a topical issue that impacts many organisations. Many of these organisations have not fully come to grip with the actual implications to the business or understand how employees are dealing with this on a day to day basis. The research is important as it will assist a selected financial institution to fill a gap in the ability to handle information management in the organisation. As highlighted previously, there are many aspects of information which companies have to cater for such as government legislation and company policies as well as marrying these two up.</p>

HOW TO COMPLETE THE INTERVIEW AND THE TARGET POPULATION
<ul style="list-style-type: none"> <li>➤ This interview questions comprises of open-ended questions which requires the respondent to verbally respond to the questions.</li> <li>➤ The interview questions are aimed at executive management in the organisation.</li> <li>➤ The questions will be asked face to face by the researcher. If the question is not understood the researcher will be on hand to explain the question.</li> <li>➤ The researcher will document all answers to the questions represented on this interview question list.</li> </ul>

CONFIDENTIALITY AND ANONYMITY
Please note that ALL information provided by any respondent will be kept strictly confidential and the anonymity of the respondent is guaranteed.

SECTION A – BIOGRAPHICAL INFORMATION	
<b>1) Gender</b>	
Male	01
Female	02X
<b>2) Age</b>	
21-30	01
31-40	02X
41-50	03
51-60	04
60-65	05
65 and above	06
<b>3) Highest level of education completed</b>	
Below matric	01
Matric	02
Diploma	03
Bcom or Btech	04
Honours	05X
Masters	06
<b>4) What staffing level can you be classified in?</b>	
Executive Management	01
Senior Management (Non Executive)	02X
<b>5) What is your current job title?</b>	
Business Centre Leader: Collections and Recoveries	
<b>6) How long have you been in this position at the company?</b>	
0 to 3 years	01X
4 to 6 years	02
7 to 10 years	03
More than 10 years	04

## SECTION B – BREACHING OF DATA IN A FINANCIAL INSTITUTION

### 7) What plans do you have to ensure that employees do not breach information in this organisation?

From our space we obviously follow the company policy. I can talk company wide and my area and the guys who report to me are pretty much aware of it. Especially when they need to send information to external vendors. If anything with a customer ID number goes out there's the alert that comes from operational risk to indicate that somebody reporting through to me has breached the policy and they've sent information out. At that point in time we'll investigate. They'll show me the initial email and its simple things like for example we don't have a FTP site where we dump information when our collectors need to be registered, so it's there ID numbers and things that goes out. Other than that it's via FTP to our external vendors,

### 8) Do you have policies in this institution dealing with information management? YES/NO

Yes, we follow company policy.

#### If YES, are they responsive or aligned to the national legislations?

Pretty much so because from a POPI (Protection of Personal Information Act) perspective we need to make sure that whenever data leaves the company it leaves in a secured mode, secured method. From a process we have in place from an IT perspective that it has to be a vendor that has a NDA (Non-Disclosure Agreement) signed with us and known with us based on that I'm pretty comfortable.

#### What are the opportunities and challenges brought by this policy?

Yes, there are. It can be labour intensive. Let's say for example we ready to go we got the data available then perhaps the FTP site has not been sorted or the vendor doesn't have access to the FTP site. As good as it is and I understand that we need to supply data there are challenges that things can't always happen.

#### If NO/YES, what are your organizational plans in place to ensure that your key stakeholders (employees and vendors etc.) do not breach information?

That's the FTP and we make it very clear to, especially new vendors coming on board, we make that very clear to them. We've just on boarded a number of EDC's (External Debt Collector) in our space as well and yes there's been a lag in getting the information through to them but it's around making sure we access the right information and that we also very clear

around what we share and what we don't share. The vendor normally is very much in line with that and then also for access to FTP sites has to be signed off.

**What tools do you have in place to ensure that your key stakeholders do not breach information?**

FTP sites are used.

## **SECTION C – INFORMATION MANAGEMENT MITIGATION IN A FINANCIAL INSTITUTION**

**9) Do you have, in this organization, mitigation strategies on information management?**

**YES/NO**

Yes.

**10) What are your mitigation plans in relation to information management?**

Before we were very loose and we could just send data and information out. Now with all the processes in place we've become more stringent around what we share and what's not shared. Can it be enhanced? I think so because there's alerts that come through regularly and some of those things are communicated to the debt collector's council. They are not going to access our FTP site so for every time that information is shared I'm going to get an alert so I do think there are very specific vendors where we know our information has to go out where we know there is no FTP site that there should be a list somewhere and where we see that breach coming through from a particular person we should know what it is.

**11) Are staff members, other than executive management, aware and knowledgeable of the information management security policies put in place by the organisation? YES/NO**

Yes.

**a) If yes, what is done in order to achieve this?**

Staff are aware, staff awareness. For staff members anything that is generated at a customer level perspective is generated via our collections and debtor systems and that is normally secure. Those are via email. That's communication between the customer and it comes from a central mailbox. If there is individual stuff that goes out from a personalized mailbox, company mailbox, that would get an alert and the staff are aware of that. The other stuff all goes via the Collections mailboxes for communication.

**b) If no, what does the organisation view as the being important in relation to information management?**

## **SECTION D – INFORMATION MANAGEMENT PREPAREDNESS IN A FINANCIAL INSTITUTION**

**12) Do you have preparedness plans to respond to any potential risk on information management? YES/NO**

Going forward in future, no, and don't know if as a business if they've got things in place.

- a) How are government policies and regulations on information management aligned with this organisations policies?**
  
- b) If it's not aligned, what are the organisations view on the future state to align this?**

## **SECTION E – INFORMATION MANAGEMENT SYSTEMS IN A FINANCIAL INSTITUTION**

**13) How are the organisations technology systems aligned to the strategic plans of the organisation in relation to information management?**

Other than the processes we have in place, first of all information cannot be sent off directly from anyone of the systems in my area. It needs to be via an extract which already is dumped on an FTP site. From that perspective nothing from the system as such.

- a) If it's not aligned, why?**

## **SECTION F – RISK RESPONSE AND RECOVERY IN A FINANCIAL INSTITUTION**

**14) What are the organisations risk management plans to deal with information management breaches?**

There's the alert that goes and that alert is sent to the line manager then I normally would respond directly to the operational risk manager and say there was a breach from that person's mailbox, this is where it went to and this is the reason why it went out via email.

## **APPENDIX C: HYPOTHESIS TESTING**

Attached as an excel document.

## **APPENDIX D: CORRELATIONS**

Attached as an excel document



## APPENDIX E: ROTATED COMPONENT MATRIX

### Rotated component matrix for breaching of data in a financial institution

BREACHING OF DATA IN A FINANCIAL INSTITUTION	Component		
	1	2	3
I ensure that I do not breach confidential information	.861	.258	.113
I ensure that I secure organisational personal information	.882	.202	.093
I make sure that I don't breach security information	.877	.081	.022
I'm not associated in fraudulent activities	.816	.124	-.048
My activities are aligned to government regulations	.594	.176	-.177
There are no occurrences of information breaches	.580	.200	.005
Data breaches has a positive impact	-.035	-.034	.722
Customers are not concerned about information management	.127	.161	.651
Breaching of information is assessed	.244	.783	.091
Employees are trained on information security policies	.033	.843	.073
Experienced employees are more compliant on security policies	.289	.002	.489
Employees keep customer information confidential	.292	.732	.017
Employees are held accountable for breaching customer data	.233	.658	.124
Data breaches do not affect its economic condition	-.121	.065	.845
Data breaches only occur accidentally	-.175	.106	.544

Extraction Method: Principal Component Analysis.

Rotation Method: Varimax with Kaiser Normalization.<sup>a</sup>

a. Rotation converged in 5 iterations.

### Rotated component matrix for information management mitigation in a financial institution

INFORMATION MANAGEMENT MITIGATION IN A FINANCIAL INSTITUTION	Component			
	1	2	3	4
Information management security policies are in place	.182	.038	.696	-.084
Information management programmes are in place to educate employees	.789	.067	.381	-.117
There is low risk of information breaches	-.055	.798	.024	-.044
Information is protected from the moment it is created until the end of its cycle	.533	.446	-.278	-.432
I have access to customer information that is not a necessity to perform my job	.050	.020	-.157	.884
I have attended information management training which is beneficial to me	-.083	.155	.638	-.066
Information management risks are managed well	.287	.513	.517	-.254
Risk assessments are done in order to quantify threats	.297	.511	.176	.254
Management plays an important role to promote information security	.401	.241	.574	.200
Money is spent to mitigate data breaches	.346	.644	.257	.091
Information security is part of my organisational culture	.190	.596	.424	-.296
There are awareness campaigns on information security	.655	.354	.371	.121
Employees' knowledge is regularly tested on information security policies and procedures	.851	.095	-.053	.057

Extraction Method: Principal Component Analysis.

Rotation Method: Varimax with Kaiser Normalization.<sup>a</sup>

a. Rotation converged in 7 iterations.

### Rotated component matrix for information management preparedness in a financial institution

INFORMATION MANAGEMENT PREPAREDNESS IN A FINANCIAL INSTITUTION	Component	
	1	2
I am aware of government regulations and procedures on information management	.045	.836
Employees are the strongest link in information security	.211	.679
If data breaches do occur there is a set procedures in place that I will follow	.873	.075
Information management security is part of my institutional culture	.737	.148
Policies on information management are clear	.781	.191
There are disciplinary measures in place to address employee negligence on information management	.760	.046
Information security forms part of the annual organisations budgeting	.672	.337

Extraction Method: Principal Component Analysis.

Rotation Method: Varimax with Kaiser Normalization.<sup>a</sup>

a. Rotation converged in 3 iterations.

### Rotated component matrix for information management systems in a financial institution

INFORMATION MANAGEMENT SYSTEMS IN A FINANCIAL INSTITUTION	Component		
	1	2	3
Technology based solutions are all that is required to ensure information security	.402	.481	.332
Without IT systems we cannot control information management	.519	.234	.220
The software systems I use have strict access control to customer information	.746	-.114	-.092
The IT systems are aligned with the requirements of protecting customer information	.830	-.028	-.022
Data protection and security protection controls are in place on computers	.690	-.104	-.007
Employees have access to pass customer information to a third party. E.g. via email	-.215	.863	-.081
All interactions with customers are recorded on an IT system	.664	.320	-.273
The IT area is well informed of necessities related to privacy regulation and policies	.810	-.059	-.241
The standard of information security systems are assessed against international accepted rules and practises	.726	-.008	-.006
Employees are required to demonstrate to consumers their level of compliance in relation to information security guidelines	.719	.194	.253
All business stakeholders are involved when implementing IT systems	.657	.064	.013
Information systems are becoming more exposed to risk and breaches	-.127	-.017	.885

Extraction Method: Principal Component Analysis.

Rotation Method: Varimax with Kaiser Normalization.<sup>a</sup>

a. Rotation converged in 6 iterations.

### Rotated component matrix for risk response and recovery in a financial institution

RISK RESPONSE AND RECOVERY IN A FINANCIAL INSTITUTION	Component		
	1	2	3
Information risk management is not important	.122	.801	-.040
Risk management does not need to form part of a business strategy	.071	.851	.054
The requirement for risk management is on the decrease	-.037	.410	.716
Regulatory risks should not form part of the institution's risk plan	.140	.761	.271
There are no controls in place to react to information management risks	.619	.323	.209
We do not respond well to risks on information management	.838	.100	.122
There are no contingency plans in place to deal with risks on information management	.822	.208	.180
Information is not securely backed up in the event it should be lost	.647	-.247	.469
I am not able to identify information risks	.444	.085	.707
I reactively respond to information risks	.094	-.008	.666
There are instances when I do not get notifications on information risks	.639	.031	-.044

Extraction Method: Principal Component Analysis.

Rotation Method: Varimax with Kaiser Normalization.<sup>a</sup>

a. Rotation converged in 5 iterations.

## APPENDIX F: CHI-SQUARE TEST

### Chi-square test of breaching of data in a financial institution

	Chi-Square	df	Asymp. Sig.
I ensure that I do not breach confidential information	144.519	2	0.000
I ensure that I secure organisational personal information	144.519	2	0.000
I make sure that I don't breach security information	150.222	2	0.000
I'm not associated in fraudulent activities	77.049	1	0.000
My activities are aligned to government regulations	87.63	2	0.000
There are no occurrences of information breaches	45.852	2	0.000
Data breaches has a positive impact	40.519	2	0.000
Customers are not concerned about information management	22.889	2	0.000
Breaching of information is assessed	40.074	2	0.000
Employees are trained on information security policies	62.741	2	0.000
Experienced employees are more compliant on security policies	38.889	2	0.000
Employees keep customer information confidential	57.556	2	0.000
Employees are held accountable for breaching customer data	68.519	2	0.000
Data breaches do not affect its economic condition	35.852	2	0.000
Data breaches only occur accidentally	48.222	2	0.000

### Chi-square test of information management mitigation in a financial institution

	Chi-Square	df	Asymp. Sig.
Information management security policies are in place	122.889	2	0.000
Information management programmes are in place to educate employees	54.889	2	0.000
There is low risk of information breaches	3.852	2	0.146
Information is protected from the moment it is created until the end of its cycle	1.556	2	0.459
I have access to customer information that is not a necessity to perform my job	22.296	2	0.000
I have attended information management training which is beneficial to me	16.074	2	0.000
Information management risks are managed well	22.296	2	0.000
Risk assessments are done in order to quantify threats	28.074	2	0.000
Management plays an important role to promote information security	53.852	2	0.000
Money is spent to mitigate data breaches	32.667	2	0.000
Information security is part of my organisational culture	42.741	2	0.000
There are awareness campaigns on information security	32.074	2	0.000
Employees' knowledge is regularly tested on information security policies and procedures	2.000	2	0.368

### Chi-square test of information management preparedness in a financial institution

	Chi-Square	df	Asymp. Sig.
I am aware of government regulations and procedures on information management	46.889	2	0.000
Employees are the strongest link in information security	72.667	2	0.000
If data breaches do occur there is a set procedures in place that I will follow	46.222	2	0.000
Information management security is part of my institutional culture	49.852	2	0.000
Policies on information management are clear	33.556	2	0.000
There are disciplinary measures in place to address employee negligence on information management	68.963	2	0.000
Information security forms part of the annual organisations budgeting	24.889	2	0.000

### Chi-square test of information management systems in a financial institution

	Chi-Square	df	Asymp. Sig.
Technology based solutions are all that is required to ensure information security	35.630	2	0.000
Without IT systems we cannot control information management	60.963	2	0.000
The software systems I use have strict access control to customer information	50.074	2	0.000
The IT systems are aligned with the requirements of protecting customer information	58.741	2	0.000
Data protection and security protection controls are in place on computers	103.630	2	0.000
Employees have access to pass customer information to a third party. E.g. via email	33.852	2	0.000
All interactions with customers are recorded on an IT system	45.852	2	0.000
The IT area is well informed of necessities related to privacy regulation and policies	39.407	2	0.000
The standard of information security systems are assessed against international accepted rules and practises	34.741	2	0.000
Employees are required to demonstrate to consumers their level of compliance in relation to information security guidelines	18.296	2	0.000
All business stakeholders are involved when implementing IT systems	3.852	2	0.146
Information systems are becoming more exposed to risk and breaches	9.556	2	0.008

### Chi-square test of risk response and recovery in a financial institution

	Chi-Square	df	Asymp. Sig.
Information risk management is not important	144.519	2	0.000
Risk management does not need to form part of a business strategy	138.963	2	0.000
The requirement for risk management is on the decrease	53.407	2	0.000
Regulatory risks should not form part of the institution's risk plan	118.222	2	0.000
There are no controls in place to react to information management risks	56.519	2	0.000
We do not respond well to risks on information management	48.222	2	0.000
There are no contingency plans in place to deal with risks on information management	42.889	2	0.000
Information is not securely backed up in the event it should be lost	41.185	2	0.000
I am not able to identify information risks	53.407	2	0.000
I reactively respond to information risks	0.667	2	0.717
There are instances when I do not get notifications on information risks	2.296	2	0.317

## APPENDIX G: ETHICAL CLEARANCE



P.O. Box 1906 • Bellville 7535 South Africa • Tel: +27 21 6801680 • Email: saliefa@cput.ac.za  
Symphony Road Bellville 7535


Office of the Chairperson Research Ethics Committee	Faculty: <b>BUSINESS</b>
--	--------------------------

At a meeting of the Research Ethics Committee on 17 June 2015, Ethics Approval was granted to ADONIS, Mogamat Ridoh (205046924) for research activities Related to the MTech/DTech: MTech: BUSINESS ADMINISTRATION at the Cape Peninsula University of Technology

Title of dissertation/thesis:	An empirical investigation into the information management systems at a South African financial institution  Supervisor: Dr B Ngcamu
-------------------------------	--

Comments:

Decision: **APPROVED**

	17 June 2015
Signed: Chairperson: Research Ethics Committee	Date

	03/11/2015
Signed: Chairperson: Faculty Research Committee	Date

Clearance Certificate No | 2015FBREC260

## APPENDIX H: PROFESSIONAL EDITING CERTIFICATE

23 Elfin Glen Road, Nahoon Valley Heights, East London, 5200



To whom it may concern:

This document certifies that the dissertation whose title appears below has been edited for proper English language, grammar, punctuation, spelling, and overall style by Rose Masha, a member of the Professional Editors' Group whose qualifications are listed in the footer of this certificate.

Title:

An empirical investigation into the information management systems at  
a South African financial institution

Author:

RIDOH ADONIS

Date Edited:

09 June 2016

Signed:

A handwritten signature in black ink, appearing to read "Rose Masha".

Rose Khanyisile Masha

082 770 8892

Bachelor of Library and Information Science, Hons (English Language Teaching), HDE,  
MA (Hypermedia in Lang. Learning), PhD (Education).

**APPENDIX I: TURN IT IN CONFIRMATION**

# Ridoh Adonis Thesis

*by* Ridoh Adonis

---

<b>FILE</b>	R_ADONIS_THESIS_ALL_CHAPTERS_V4_-_CONDENSED.DOCX (217.44K)		
<b>TIME SUBMITTED</b>	07-JUN-2016 11:50AM	<b>WORD COUNT</b>	47145
<b>SUBMISSION ID</b>	682128508	<b>CHARACTER COUNT</b>	267292