Cyber risk management frameworks for the South African banking industry

By

CAROLINE KOTO

201113033

Limited scope dissertation submitted in fulfilment of the requirements for the degree

MAGISTER COMMERCII

In

Computer Auditing

in the

COLLEGE OF BUSINESS AND ECONOMICS
at the

UNIVERSITY OF JOHANNESBURG

Supervisor: Belinda Schutte

Co-supervisor: Rozanne Smith

2019

DECLARATION

I certify that the *limited scope dissertation* submitted by me for the degree *Master's of commerce (Computer Auditing)* at the University of Johannesburg is my independent work and has not been submitted by me for a degree at another university.

CAROLINE KOTO

(Name in block letters – no signature)

ACKNOWLEDGEMENTS

I wish to extend my heartfelt gratitude to the following people who contributed to the successful completion of this limited scope dissertation:

- My sister, Matlhodi Koto, thank you for being a shoulder to cry on when this journey got emotionally draining, dark and lonely. You have been a strength. Thank you for your continued love and support;
- My best friend, Nele Matshika. I cannot thank you enough for being there for me every step of the way. Thank you for all the late nights you stayed up with me and not allowing me to give up. Your presence, love and support made this journey more bearable. You are a pillar;
- My colleagues and friends, Obakeng Lengana, James Matlala, Mafusi Lephoto and Amanda Mhlongo. Thank you that you never ceased to encourage me and celebrate every little progress I made. Special thanks to Obakeng Lengana for always availing yourself when I needed your help. I value every advice and remark you contributed;
- My supervisor, co - supervisor, and former supervisor, Belinda Schutte, Rozanne Smith and Lyndsay Maseko respectively. Thank you for your effort in helping me achieve this mile stone. I have learnt so much from you. Your work ethic is incredibly strong and desirable;

Above all, I give all glory and honour to the Almighty God, who afforded me this opportunity, granted me the grace and strength to successfully complete this limited scope dissertation and blessed me with everyone who supported me through it. None of this would be possible without you. HALELLUJAH!

ABSTRACT

Information technology (IT) has proven to be critical in the operation of businesses today. The banking industry is one of the industries that are most reliant on IT. The banking industry has enjoyed greater efficiency and effectiveness in their operations owing to the widespread use of IT. However, due to IT and continuous technological advancements, new threats such as cyber risk have surfaced, and the banking industry has experienced the most cybercrime incidents. In addition to the banking industry being the most targeted by cyber-criminals, cybercrime incidents have detrimental impacts on the industry. As a result, it is crucial for banks to employ effective cyber risk management processes.

The South African banking industry is required by the South African Reserve Bank (SARB) to align their cyber risk management processes to the cyber resilience guidance document issued by the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO). The CPMI–IOSCO cyber resilience guidance contains guidelines that should be addressed within a bank's cyber risk management framework. This study seeks to establish whether the Improving Critical Infrastructure Cybersecurity (ICIC) framework addresses the guidelines contained in the CPMI–IOSCO cyber resilience guidance. The ICIC framework is effective for managing cyber risk and allows an organisation to modify it to suit its specific needs and objectives. The objective of the study is to recommend to the South African banking industry, a framework for managing cyber risks that is effective and that addresses the CPMI–IOSCO cyber resilience guidelines. The results were gathered by analysing the ICIC framework and mapping it against the CPMI–IOSCO cyber resilience guidelines.

The results revealed that the ICIC framework addresses up to 71 percent of the CPMI –IOSCO cyber resilience guidelines. The study therefore recommends that instead of building a new cyber risk management framework, the South African banking industry should adopt the ICIC framework and modify it by adding the 29 percent of the CPMI –IOSCO cyber resilience guidelines not addressed by the ICIC framework. All the guidelines contained in the CPMI–IOSCO cyber resilience guidance will then be addressed within the modified ICIC framework. South African banks will also achieve effective management of cyber risks through the ICIC framework.

Keywords

Cybercrime

Banking industry

Cyber risk management

ICIC framework

Cyber resilience guidance

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ATM	Automated Teller Machines
BIS	Bank for International Settlements
CPMI	Committee on Payments and Market Infrastructures
DDoS	Distributed Denial of Services
DNS	Domain Name System
EFT	Electronic Fund Transfer
FINTECH	Financial Technology
FMI	Financial Market infrastructures
HTTP	Hypertext Transfer Protocol
ICIC	Improving Critical Infrastructure Cybersecurity
ICT	Information Communications Technology
IOSCO	International Organization of Securities Commissions
IRC	Internet Relay Chat
IT	Information Technology
NIST	National Institute of Standards and Technology
SARB	South African Reserve Bank
SIFMA	Securities Industry and Financial Markets Association
SMS	Short Message Service
U.S.A	United States of America

CHAPTER ONE

INTRODUCTION AND LAYOUT

1.1 INTRODUCTION

Businesses are continuously exposed to risks, and thus it is vital for them to identify the risks they are exposed to and to manage them effectively (Asgary, 2016; Giahi, Sahebjamnia & Torabi, 2016; Hopkin, 2017). In the event that a risk materialises, effective risk management plays the role of keeping the impact of that risk to a minimum (Wong & Shi, 2015). While some risks have a low impact on business, others can lead to the discontinuation of main business functions, a complete shutdown of the entire business, or even great financial losses (Ashford, 2016; Hopkin, 2017). Among the risks that have high impacts, Information Technology (hereafter, IT) risks are the most pervasive (Berisha-Shaqiri, 2015; Giahi *et al*., 2016; Asgary, 2016). Businesses have grown very reliant on IT to a point where if an IT system fails, the business could have their main business functions interrupted and large amounts of money could be lost (Berisha-Shaqiri, 2015; Marx & Hohls-du Preez, 2017).

The banking industry has most of its functions supported and maintained by IT (Bishnoi & Devi, 2017). The industry has gone through a drastic transformation in order to improve its service delivery capacity, and IT played a big role in achieving this (Harguem & Echatti, n.d). The role of IT in the banking industry is continuously advancing and is expected to advance at an increasing rate in the future (Lata, 2016). With IT in banking increasingly advancing, banks are pressed to invest most of their capital expenditure on IT (Sattar, 2014; Yadurvedi, 2015; Flinders, 2017).

IT capital expenditures by banks have resulted in several benefits enjoyed by the industry (Binuyo & Aregbeshola, 2014; Eruemegbe, 2015). Banks are now able to facilitate network transactions, save on expenses, save time, improve organisational performance and have achieved upward shifts in profits because of IT (Eruemegbe, 2015; Maryam, Khamesi & Houshang, 2016). IT has however exposed the banking industries to new risks and if these are not effectively managed, main business functions could be interrupted, leading to great financial losses (Deloitte, 2016; Marx & Hohls-du Preez, 2017). In order for business in the banking industry to continue uninterrupted, the industry does not have the option of getting rid of IT but instead must employ effective IT risk management tools (Lata, 2016).

1.2 IT IN THE BANKING INDUSTRY

The banking industry as currently understood, has been redefined and re-structured due to the widespread use of IT in its business processes (Tiwari & Kumar, 2012). Before the widespread use of IT, customers would stand in long queues to withdraw their money, and banks used to create handwritten receipts as well as keep large numbers of general ledger books (Agrawal, 2016; Sravanthi, 2016; Korte, 2017). With the use of technology, banks have improved their functions as well as the services they provide (Dandago & Rufai, 2014; Bishnoi & Devi, 2017). An increased use of IT is envisaged in future due to continuous innovations (Gupta & Chanava, 2013). Moreover, banks are already pursuing the latest emerging technologies and continuing to be innovative (Yadurvedi, 2015).

Examples of technological innovations that have emerged in banking are Automated Teller Machines (hereafter, ATMs), Electronic Fund Transfers (hereafter, EFT), debit cards, mobile banking, credit cards, tele-banking, e-banking, the establishment of call centres and many more (Sattar, 2014; Yadurvedi, 2015; Lata, 2016). Most of these innovations have resulted in banks' heavy utilisation of payment systems that are IT enabled, have internet-based access and new modes of delivery to extend their services and manage their fast-increasing customer needs (Harguem & Echatti, n.d). It is almost impossible to find a function in a bank or a bank product that is independent of technology, and it is for this reason that large amounts of money are expended on IT (Mclean, 2013; Deloitte, 2016; Flinders, 2017). In 2016, investment banks in the United States of America (hereafter, U.S.A) invested R132.43 billion in technology, spending R90.61 billion on supporting existing IT facilities in their organisations, and the remainder on new technologies (Flinders, 2017).

Banks are advancing mainly as a result of technology, and technological advancements in banks have resulted in convenience, speed and time-saving methods of carrying out business (Lata, 2016). Some of the more positive impacts evident in the banking industry and attributable to IT are: banks are experiencing increased profits, competitiveness, marketability and improved organisational performance (Marinč, 2013; Eruemegbe, 2015; Maryam *et al*., 2016). However, in order for the industry to completely enjoy the positive impacts of technology, they need to pay careful attention to IT risks (Svatá & Fleischmann, 2011; Lata, 2016).

IT risks in the banking industry range from strategic, operational and reputational risks (Sravanthi, 2016; Miyake, 2016). An expansion of these risks includes unauthorised transactions, processing errors, destroyed files, data theft, degraded or incapacitated systems, obsolete technologies, coordinated service attacks, disruption of key business processes outsourced to vendors, internet manipulation and cybercrime (Eruemegbe, 2015; Bevan, Ganguly, Kaminski & Rezek, 2016). Cybercrime is the most common, frequent and significant IT risk in the banking industry (Mawudor, Kim & Park, 2015)

1.3 BACKGROUND TO THE RESEARCH PROBLEM

The banking industry is faced with the highest number of cybercrime incidents compared to other business industries (Stechyshyn, 2015; Camillo, 2016; Miyake, 2016). In the year 2015 alone, the banking industry lost an average of R188.19 million due to cybercrime incidents (Camillo, 2016). Cyber-criminals also drained R44.3 million from 9 000 Tesco bank's current accounts in just one month (Ashford, 2016; Cox & Lahti, 2017). In June 2014, cyber-criminals managed to launch malicious programs and stole sensitive information from the U.S.A's biggest bank, JP Morgan Chase (Stechyshyn, 2015).

Cybercrime is a technology enabled crime, the core of which is represented by acts against the integrity, availability and confidentiality of computer information (United Nations Office on Drugs & Crime, 2013). Bank exposure to the risk of cybercrime is due to the complexity and intense utilisation of IT systems and technologies such as internet banking, mobile banking, digital wallets and ATMs (Ashford, 2016; Korte, 2017). With the fast-growing technologies and increasing usage of IT in banking, cyber-criminals will have more platforms to attack banks, and the nature of cybercrime in banking will continue to evolve (UNODC, 2013; Stechyshyn, 2015). For that reason, it is important for banks to carefully address this evolving threat of cybercrime (Stechyshyn, 2015; Standard Bank, 2017; Deloitte, 2018).

Most South African banks had cybercrime listed as one of the major risks in their annual integrated reports for the 2017 financial period (Binuyo & Aregbeshola, 2014; Nedbank, 2017). In the same year, the South African Banking Risk Information Center reported that South African banks encountered 13 438 cybercrime incidents in total, which led to losses amounting to more than R250 million (Smith, 2018; Kgosana,

2018). As a result, they have prioritised continuously improving cyber risk management processes in order to effectively manage cyber risk (Standard Bank, 2017; Nedbank, 2017; First Rand Bank, 2017). These efforts by South African banks to counter cybercrime are evidenced by the considerable amounts of money expended on cyber risk management (Deloitte, 2018).

In May 2017, the South African Reserve Bank (hereafter, SARB), through the office of the Registrar of Banks, issued a guidance note in terms of section 6(5) of the Banks Act 94 of 1990 (SARB, 2017). In this guidance note, the SARB required all South African banks to align their cyber risk management processes to the cyber resilience guidance issued by the Committee on Payments and Market Infrastructures (hereafter, CPMI) and the International Organization of Securities Commissions (hereafter, IOSCO), known as the CPMI–IOSCO cyber resilience guidance for Financial Market Infrastructures (hereafter, FMI) (Securities Industry & Financial Markets Association (hereafter, SIFMA), 2016; Standard Bank, 2017). The CPMI–IOSCO cyber resilience guidance is the latest international best practice relating to cyber risk management for banks (SIFMA, 2016; Deloitte, 2018). On a regular basis, the office of the Registrar of Banks will assess the appropriateness and adequacy of the South African banks' cyber risk management processes based on the CPMI–IOSCO cyber resilience guidance (SARB, 2017). The CPMI–IOSCO cyber resilience guidance contains guidelines that should be addressed within a bank's cyber risk management framework (Bank for International Settlements (hereafter, BIS) & International Organization of Securities & Commissions, 2016). It is therefore important for the banking industry to have a framework in place that is specifically designed to manage cyber risks (Kopp, Kaffenberger & Wilson, 2017).

A framework currently adopted by banks in South Africa is BASEL III (Standard Bank, 2012; Barclays, 2017). The challenge with the BASEL III framework is that it is not specific to cyber risks, but is generic to overall risks (Svatá & Fleischmann, 2011; Kopp *et al*., 2017). The Improving Critical Infrastructure Cybersecurity (hereafter, ICIC) framework on the other hand, is designed to specifically manage cyber risks (National Institute of Standards & Technology (hereafter, NIST), 2014). The ICIC framework was issued by the U.S.A's NIST and is widely followed by banks across the globe (Stechyshyn, 2015). This framework is commended for its efficiency as well as its

ability to be modified to suit each organisation's unique cyber risks, cyber risk tolerances, and cyber risk management objectives (NIST, 2014; Spitzner, 2017).

1.4 THE RESEARCH PROBLEM

As discussed above, it is important for South African banks to align their cyber risk management processes to the CPMI–IOSCO cyber resilience guidance, thus they must adopt a cyber risk management framework that is not only effective, but also addresses the guidelines contained in the CPMI–IOSCO cyber resilience guidance. Therefore, this study seeks to establish whether the ICIC framework addresses the CPMI–IOSCO cyber resilience guidelines.

Problem statement
To establish whether the ICIC framework addresses the guidelines contained in the CPMI–IOSCO cyber resilience guidance.

1.5 RESEARCH OBJECTIVES

The aim of this study was to establish whether the ICIC framework addresses the guidelines as set out in the CPMI–IOSCO cyber resilience guidance. In order to achieve the aim of this study, the following objectives were to be met:

- To identify and explain cyber risks that the banking industry is exposed to as well as the need for effective cyber risk management methods in the banking industry;
- To discuss the framework currently adopted by South African banks to manage cyber risks;
- To understand the ICIC framework and the CPMI–IOSCO cyber resilience guidance;
- To map the ICIC framework against the guidelines contained in the CPMI–IOSCO cyber resilience guidance; and
- To recommend to the South African banking industry, a framework for managing cyber risks that is effective and addresses the guidelines contained in the CPMI–IOSCO cyber resilience guidance.

The objectives of this study were achieved through a literature review (Chapter 2–3) on cyber risks and cyber risk management in the banking industry, as well as the ICIC

framework and CPMI–IOSCO cyber resilience guidance. Chapter 4 shows the ICIC framework mapped against the CPMI–IOSCO cyber resilience guidelines.

The ICIC framework was mapped against the guidelines contained in the CPMI–IOSCO cyber resilience guidance because:

- CPMI–IOSCO cyber resilience guidance is the latest (it was issued in the year 2016) international best practice relating to cyber risk management for the banking industry; and
- South African banks are requested by the SARB to align their cyber risk management processes to the CPMI–IOSCO cyber resilience guidance.

The results deduced from the study are summarised in Chapter 5.

1.6 SCOPE AND LIMITATIONS

- The scope is limited to discussing cyber risks and not all IT risks.
- The study discusses the impacts of cyber risks only on the banking industry.
- Currently, the South African banks have adopted the BASEL III framework. This study discusses BASEL III and the ICIC framework, however, the BASEL III will not be mapped. Only the ICIC framework is mapped against the CPMI–IOSCO cyber resilience guidelines.
- A second reviewer on the data being analysed and the mapping will not be included.

1.7 RESEARCH DESIGN AND METHODOLOGY

1.7.1 Research design

A research design refers to a plan followed in solving the research problem (Klopper, 2008). It is therefore important for the research design to be linked to the research objectives, which are formulated from the research problem (O'Leary, 2004). A research design should address the data needed and the methods the researcher adopts to gather and analyse that data, in order to achieve the research objectives (Kothari, 2004).

The objectives of this research aim to establish whether the ICIC framework addresses the guidelines as set out in the CPMI–IOSCO cyber resilience guidance. They also aim to identify and explain the cyber risks and their impact that the banking industry is

exposed to, and the need for effective cyber risk management methods in the banking industry.

In order to achieve the above-mentioned research objectives, the researcher adopted the qualitative approach whereby the data extracted from the content analysis contains secondary data. The qualitative approach to research relates to subjective evaluation of a research phenomenon (Kothari, 2004). This approach is usually used to extract secondary data (O'Leary, 2004). The secondary data is gathered from textbooks, publications, the internet, online journal articles, and the online library of the University of Johannesburg.

In the qualitative approach, phenomenology, grounded theory, phenomenographic, hermeneutics, ethnography and content analysis are the different techniques used for analysing data (Bengtsson, 2016). Content analysis is the technique that formed the research design for the purposes of this study. Content analysis is a technique whereby the researcher analyses existing documents to test theoretical subjects in order to enhance understanding of the data collected (Elo & Kyngäs, 2007).

1.7.2 Research methodology

Research methodology is a systematic process by which the researcher solves a research problem (Kothari, 2004). It refers to the science relating to how research is going to be conducted (Sahu, 2013). In describing research methodology, the researcher must articulate the various steps adopted in solving the research problem (Kothari, 2004). In this research process, the adopted steps were as follows:

Step 1: Identify the research problem

The identified research problem relates to the CPMI–IOSCO cyber resilience guidance and the guidelines contained therein. The research problem is to establish the ICIC framework addresses the guidelines as set out in the CPMI–IOSCO cyber resilience guidance

Step 2: State the research objectives

The research objectives, as outlined in section 1.5, were derived through a thorough enquiry to understand the problem.

Step 3: Review the literature

Literature is made up of written sources relevant to the study field the researcher has chosen (Klopper, 2008). The relevant literature review can be found in Chapters 2 and 3. These chapters inform the readers of cyber risks and their impact on the banking industry, and the need for effective cyber risk management methods. These chapters also inform the reader of the risk management framework that South African banks have currently adopted and discuss the ICIC framework and the CPMI–IOSCO cyber resilience guidance. The research in these chapters was conducted by gathering secondary data.

Step 4: Prepare the research design

The research design adopted in this research is explained in section 1.7.1.

Step 5: Sample design and sample selection

A population consists of all the items under consideration in a research field (Kothari, 2004). In order to generalise the results of the research, a representative sample must be selected from the population (O'Leary, 2004). A sample refers to a few items selected from a population (Klopper, 2008). The process through which the researcher selects a sample from a population is referred to as a sample design (Kothari, 2004).

For the purposes of this study, the population was identified as all the risk management frameworks for the banking industry. For the selection of the sample, a non-probability sampling design was adopted. In this design, the researcher deliberately and purposefully selects a sample from the population by applying own judgment (Kothari, 2004). The selected sample in this study was the ICIC framework. The researcher deliberately and purposefully selected this framework for the following reasons:

- It is not a framework generic to all risks, but a framework for specifically managing cyber risks (Svatá & Fleischmann, 2011; Spitzner, 2017);
- It is flexible and efficient for managing cyber risk, which is vitally important for the banking industry (Roman, 2014; Clozel, 2016); and
- It is widely adopted by banks across the globe (Stechyshyn, 2015).

Step 6: Collect the data

The researcher aimed to collect data through a qualitative approach. The literature was collected from textbooks, publications, the internet, online journal articles, and the online library of the University of Johannesburg. In the literature, the researcher aimed to find different cyber risks and their impacts on the banking industry, the risk management framework currently adopted by the South African banking industry, and the ICIC framework and the CPMI–IOSCO cyber resilience guidance.

Step 7: Analyse the data

For this study, a qualitative content analysis procedure was followed. During this process, the ICIC framework and the CPMI–IOSCO were analysed. The analysis was done in order to establish the ICIC framework addresses the guidelines as set out in the CPMI–IOSCO cyber resilience guidance. To establish this, the ICIC framework practices were compared against each guideline in the CPMI–IOSCO cyber resilience guidance. This process takes place in Chapter 4.

Step 8: Interpret the data

During the interpretive process, the results of the study were scrutinised. From the analysis, the researcher determined which CPMI–IOSCO cyber resilience guidelines are addressed by the ICIC framework. The interpretation of the data informed on the following possibilities:

- The ICIC framework addresses none of the CPMI–IOSCO cyber resilience guidelines;
- The ICIC framework addresses some of the CPMI–IOSCO cyber resilience guidelines; or
- The ICIC framework addresses all of the CPMI IOSCO cyber resilience guidelines.

The data interpretation could facilitate the South African industry to decide whether to adopt the ICIC framework in order to be aligned to the CPMI–IOSCO cyber resilience guidance, as required of them by the SARB.

1.7.3 Ethical considerations

Ethical considerations refer to ensuring that the rights of research participants are protected, informed consent is obtained, and that ethical approval has been obtained from the institution following the institutional ethics review process (Klopper, 2008). Careful consideration regarding all ethical concerns was taken for this study. Ethical clearance by the University of Johannesburg's School of Accountancy Research Ethics Committee was granted. The ethical clearance report is attached at the end of this study. Moreover, the sources used throughout this research have been acknowledged by referencing them according to the UJ Harvard referencing method.

1.8 CHAPTER OUTLINE

Chapter one: Introduction and layout

In this chapter the background to the research, the problem statement and the research objectives are discussed. The research design and methodology is also addressed in this chapter.

Chapter two: Cyber risks and cybersecurity in the banking industry

This chapter provides the cyber risks that the banking industry is faced with as a result of its heavy reliance on IT. The chapter also studies the impact of these cyber risks on business in the banking industry. Furthermore, the chapter discusses the need for effective cyber risk management measures in the banking industry.

Chapter three: Risk management frameworks and the CPMI–IOSCO cyber resilience guidance

This chapter discusses the risk management framework currently adopted by the South African banking industry, namely BASEL III. The chapter analyses the ICIC framework issued by NIST and the CPMI–IOSCO cyber resilience guidance for FMIs.

Chapter four: The empirical study and research findings

In this chapter, the ICIC framework is mapped against the guidelines of the CPMI–IOSCO cyber resilience guidance. In this chapter, the results of the mapping are analysed and discussed.

Chapter five: Conclusions

This chapter summarises the results deduced from the study. Thereafter, conclusions are drawn and areas for future research suggested.

1.9 CONCLUSION

This chapter discussed the importance of effectively managing the IT risks that result from the intense reliance on IT by businesses. The banking industry was highlighted as one of the industries that rely heavily on IT for the functioning of their critical functions and in the operation of most of their products. Even though technological advancements have reshaped the industry by transforming the manner in which business is conducted and improving overall organisational performance, banks face new risks as a result of IT. The impacts of these IT risks cause business interruptions and considerable financial losses. Amidst the IT risks that the banking industry is exposed to, cyber risk is the most common and the most frequent. The banking industry suffers the most cyberattacks and loses significant amounts of money as a result. The management of cyber risks is therefore an important process for the banking industry, which has, as a result, allocated considerable amounts of money towards managing cyber risks. Numerous banks across the globe follow the ICIC framework to manage cyber risk. South African banks are required by the SARB to align their cyber risk management processes to the CPMI–IOSCO cyber resilience guidance by adopting or building a cyber risk management framework that addresses the CPMI–IOSCO cyber resilience guidelines.

The following chapter enumerates different types of cyber risks and discusses their impact on the banking industry. This study also discusses cybersecurity and its importance in the banking industry.

CHAPTER TWO

CYBER RISKS IN THE BANKING INDUSTRY

2.1 INTRODUCTION

The banking industry is experiencing greater efficiency and effectiveness in their business as a result of technological advancements (Dzomira, 2014; Shackleford, 2015; Brady, 2018). However, these technological advancements have attracted threats such as cyber risks (Li, 2017; Alese, Thompson, Alowodu & Oladele, 2018). Cyber risk is the most common topic in business today and the banking industry is one of the most targeted by cyber-criminals. (Rama, 2016; Grobler, 2018; Kundu, Islam, Jui, Rafi, Hossain & Chowdhury, 2018). As a result, the banking industry has experienced the highest numbers of cyberattacks and these have been increasing at an alarming rate (Lagazio, Sherif & Cushman, 2014; Shackleford, 2015; Van Den Bergh & Pretorius, 2017).

One of the earliest documented cybercrimes, which occurred in 1958, involved an unauthorised change to bank records (Li, 2017). Till today, banks are still impacted by cyberattacks, which with time and developments in technology, have become more numerous and sophisticated (Lemieux, 2015; Brady, 2018). Moreover, cyber-criminals have a well-developed and growing market for cybercrime acts as well as the selling of cybercrime tools and techniques used to perform cybercrime activities (Lagazio *et al*., 2014). It is therefore essential that the banking industry has an understanding of cybercrime, the cybercrime risks that the industry is exposed to, the impact of their occurrence on business, and the importance of cybersecurity (Ben-Asher & Gonzalez, 2015; Pricewaterhousecoopers, 2016; Van Den Bergh & Pretorius, 2017).

2.2 DEFINING CYBERCRIME

Cybercrime can be divided into four different categories: cyber-pornography, cyber-violence, cyber-trespass and cyber-deception and theft (Alese *et al*., 2018). There are several definitions of cybercrime as construed by groups and individuals (Van Den Bergh & Pretorius 2017). The most common definition of cybercrime refers to computer related malicious acts, which include the manipulation of and damage to electronic information, unauthorised access to computer systems, software piracy, as well as physical damage to computer systems (Lagazio *et al*., 2014; Lemieux, 2015). Cybercrime not only involves malicious acts but also the misuse of the functions that

IT systems are originally designed for (Shalaginov, Johnsen & Franke, 2017). Banking institutions suffer the risk of cybercrime resulting from mischievous acts of human attackers who thrive on destroying or defrauding the target victim (Brady, 2018).

The risk of cybercrime is one of the most important risk management topics in business today (Grobler, 2018). It has been classified as an operational risk specifically in the banking industry, and it is therefore recommended that it be addressed as such (Standard Bank, 2017; First Rand, 2017; Brady, 2018). Operational risk is the risk of loss that results from deficient or unsuccessful internal processes, systems and people, or from external occurrences (Kopp *et al*., 2017). This risk is present across all business activities in the banking industry, and furthermore, banks attribute this risk as a top-ranking threat to business growth (Baker, 2015; Nedbank, 2017).

2.3 CAUSES OF CYBERCRIME

Technology has created a platform for cybercrime, and technological growth is directly linked to the increased avenues for cyberattacks (Standard Bank, 2017; Shalaginov *et al*., 2017; Kundu *et al*., 2018). The first cybercrime was committed following the creation of the first computers and even currently, cybercrime has kept pace with the technological developments that have taken place since then (McLean, 2013; Li, 2017). Technological developments have also contributed to the sophistication of perpetrators of cybercrime (Nedbank, 2017; Shalaginov *et al*., 2017; Zhijun & Ning, 2017).

This ongoing sophistication of cyber-criminals is one of the main reasons for the reported increasing number of cybercrime incidents globally (Standard Bank, 2017; Kundu *et al*., 2018). Continuous rapid growth of computer power, the rise of financial technology (hereafter, fintech), the availability of cyber weapons and increasing numbers of technological devices also contribute to this ever-increasing number of cybercrime incidents (Grobler, 2018).

Cybercrime incidents affecting more than one country at a time are caused by global connectivity and the internet (Lemieux, 2015; Gallegos-Segovia, Bravo-Torres, Larios-Rosillo, Vintimilla-Tapia, Yuquilima-Albarado & Jara-Saltos, 2017). The internet, which is one of the ways through which the world is interconnected and has the fastest growing areas of technological infrastructure development, forms an important part of businesses today (Dzomira, 2014; Kundu *et al*., 2018). As a result, it is the most

utilised platform by cybercrime perpetrators, intensifying the risk of cybercrime in business, especially in banking (Lagazio *et al*., 2014; Sarika & Varghese, 2017).

Digitisation of banks is the main cause for cybercrime in banking (Standard Bank, 2017; Kopp *et al*., 2017). According to Mohurle & Patil (2017), digitisation of banks refers to such technological advancements as mobile technology, cloud computing, artificial intelligence, advanced analytics, robotics, biometrics and fintech, which have become the core of banking (Nedbank, 2017). With the growth of digitisation and the interconnectivity of banking functions, cyber-criminals are growing more and more sophisticated, leaving the banking industry prone to cybercrime risks (Dzomira, 2014; Shackleford, 2015). The main reason that these cybercrime acts are directed towards banks is that banks keep their money in cyberspace, and the aim of cyber-criminals is always financial gain (Dzomira, 2014).

Banks operate more through various external service providers, which form part of the banks' supply chain (States News Service, 2018). A weak link in that supply chain may expose banks to cyber risks no matter how strong their cybersecurity measures are (Pricewaterhousecoopers, 2016; Mbelli & Dwolatzky, 2016). Other causes of cybercrime in banking include breaches of confidential records, running ageing systems, less control of access to cyber systems, and shortage of cybersecurity skills (Mbelli & Dwolatzky, 2016; Standard Bank, 2017). Other cybercrime causes are weaknesses in digital identity management, the ease with which false identity can be utilised, point-of-sale terminals, payment networks, inadequate cybercrime laws, and the rise of on-line banking (Dzomira, 2014; Lemieux, 2015).

A significant number of cyberattack attempts are successful in banks due to the fact that line managers and senior managers often lack oversight when it comes to deviations from the banks' existing cyber risk controls (Dzomira, 2014). The lack of IT skills and appropriate legal frameworks at national level to address cybercrime has magnified the problem of cybercrime in African countries, including South Africa (Cassim, 2011; Lagazio *et al*., 2014).

2.4 TYPES OF CYBERCRIME

The nature of cybercrime has grown sophisticated over time and businesses are yet to experience even more sophisticated cyberattacks (Shackleford, 2015; Standard Bank, 2017; Nedbank, 2017; Grobler, 2018). A common range of cybercrimes include

identity theft, malware, social engineering, distributed denial of services (hereafter, DDoS) attacks and botnets (Shackleford, 2015; Rama, 2016; Van Den Bergh & Pretorius, 2017).

Attacks to IT infrastructures as well as compromised bank cards and accounts are frequent cyberattacks in the banking industry globally (Lagazio *et al*., 2014). The cyberattacks that the South African banking industry is exposed to include cyber fraud, ATM fraud, internet fraud, digital attacks, as well as the common cyberattacks such as ransomware and phishing attacks (Standard Bank, 2017; Nedbank, 2017; Brady, 2018; Kundu *et al*., 2018). Even though Standard Bank experienced a considerable decline in the number of phishing attacks, this attack is the most frequent in South African banks (Mbelli & Dwolatzky, 2016; Standard Bank, 2017). The following sections explain the different types of cybercrimes.

2.4.1 Identity theft

Identity theft occurs when one person makes use of the identity characteristics of another without their permission (Dzomira, 2014; Minniti, 2016). Before advancements in technology, identity theft involved merely masquerading to physically look like someone else, but nowadays identity theft is mostly committed online and with malicious intent (Van Den Bergh & Pretorius, 2017). The main aim of the identity thief is to obtain and use the victim's personal information such as credit card information, identity numbers, address, usernames and passwords, for personal financial gain (Pandey, Shah, Sharma & Farik, 2016; Zaeem, Manoharan, Yang & Barber, 2017). Cyber-criminals can also steal an employee's credentials and use them to gain remote access to infiltrate and steal money from the organisation where that person is employed (Shackleford, 2015).

2.4.2 Malware

Malware is a combination of the words 'malicious' and 'software' (Rama, 2016). With this attack, a malicious program is created to penetrate a system's software with the aim of compromising the software's integrity, confidentiality and availability by damaging, stealing and blocking access to information systems and assets (Shackleford, 2015; Minniti, 2016). These malicious programs are commonly distributed through flash drives, emails, websites and social media without the user's knowledge (Page, Jourdan, Bochmann, Flood & Onut, 2018). Types of malware

attacks include spamming, phishing, ransomware, virus, Trojan horse, worms and spyware (Mbelli & Dwolatzky, 2016; Van Den Bergh & Pretorius, 2017). Below are descriptions of the various types of malware attacks.

2.4.2.1 Spamming

Spamming is one of the common types of cybercrime and is committed by sending unwanted emails and messages to the victim (Dzomira, 2014; Pandey *et al*., 2016). These emails and messages are meant to lure victims to click on links that will allow the cyber-criminal to obtain certain personal information about the victim (Van Den Bergh & Pretorius, 2017).

2.4.2.2 Phishing

Another common type of cybercrime and the most frequent in business is phishing (Van Den Bergh & Pretorius, 2017). Phishing, just like spamming, also involves the sending of misleading emails and messages (Minniti, 2016; Baykara & Gürel, 2018). These emails and messages are disguised to look like they are from a legitimate source in order to deceive the victim into revealing their personal information such as pin codes, passwords, account numbers and authentication credentials (Rama, 2016; Jensen, Dinger, Wright & Thatcher, 2017). According to security experts, 91 percent of all cyberattacks start with phishing attacks. Moreover, it is predicted that phishing attacks are predicted to continuously grow in number and sophistication (Jensen *et al*., 2017; Sarika & Varghese, 2017).

Examples of sophisticated phishing methods are smishing and vishing (Dzomira, 2014). Smishing is a combination of phishing and Short Message Services (hereafter, SMS) (Joo, Moon, Singh & Park, 2017). This method of phishing tricks the victim by sending them an SMS that lures them into making retail payments by clicking on a link using their mobile phones, to accounts masquerading as legitimate, (Yeboa-Boateng & Amanor, 2014; Park, 2014). Vishing, on the other hand, is a method of phishing where the attacker uses a voice call to lure the victim into providing their personal details, which the attacker then uses to steal the victim's money and cause harm (Yeboa-Boateng, & Amanor, 2014; Shahriar, Klintik & Clincy, 2015).

2.4.2.3 Ransomware

This is one of the most terrible malware-based cyberattacks (Van Den Bergh & Pretorius, 2017). It is usually introduced through a phishing attack (Deloitte, 2015). When a ransomware enters a computer, the cyber-criminal is able to lock the user's access to files or computer systems with an encryption key (Gallegos-Segovia *et al*., 2017; Grant Thornton, 2017; Mohurle & Patil, 2017). The user will then receive a pop-up warning message requesting a monetary ransom in order for them to retrieve that encryption key and unblock the access (Deloitte, 2015; Pandey *et al*., 2016; Mohurle & Patil, 2017; Kundu *et al*., 2018).

Wannacry is one of the most recent types of ransomware attack, which encrypts computers, disks and files, and then demands that a ransom be paid into three bitcoin accounts within a period of three days in return for a decryption key (Mohurle & Patil, 2017; Grant Thornton, 2017). Wannacry ransomware attacks are accomplished through phishing emails that contain malicious programs (Mohurle & Patil, 2017). Petya is another type of a ransomware attack which makes use of other hacking tools to steal confidential data from a computer system, spread a malicious code to other windows system administration tools, then after an hour it reboots and encrypts the entire system or files (Ernst & Young, 2017)

2.4.2.4 Virus

Virus is a well-known cyberattack whereby an unwanted malicious code is transferred to a non-malicious computer program (Dzomira, 2014). The malicious code aims to either destroy or corrupt the program (Van Den Bergh & Pretorius, 2017).

2.4.2.5 Trojan horse

This malware-based cyberattack is sent through to a user as a misleading program that appears to be non-threatening (Marx, Schönfeldt, Watt, Van Dyk, Maré & Ramuedzisi, 2011; Van Den Bergh & Pretorius, 2017). This program imitates a legitimate program, however, it contains a malicious code and steals the victim's user credentials (Dzomira, 2014). Trojans are often installed in banking systems to record the user's keystrokes in order to capture the user's banking credentials and use them to transfer funds from the user's account to the attacker's account (Deloitte, 2015).

2.4.2.6 Worms

This malicious program is able to reproduce itself and spread to other computers connected to one network (Dzomira, 2014). It is similar to a virus, however, a worm spreads through networks while a virus can spread through any medium (Van Den Bergh & Pretorius, 2017).

2.4.2.7 Spyware

Spyware attackers trace all the digital activities of a user without their permission and knowledge (Rao & Yalamanchili, 2012). Spyware is normally disguised as legitimate software and if undetected, can restrict bandwidth, steal personal data and generate numerous pop-up messages (Van Den Bergh & Pretorius, 2017).

2.4.3 Social engineering

Social engineering attack is a method whereby cyber-criminals use social skills and psychological manipulation to deceive people into revealing personal information (Pandey *et al*., 2016; Gallegos-Segovia *et al*., 2017). Through social engineering the cyber-criminal can obtain confidential information such as company information, system access credentials, account numbers and any other sensitive information the cyber-criminal might need (Yeboa-Boateng & Amanor, 2014; Rama, 2016). One of the common ways to achieve this is to send an email to the target, making it appear as if it is from a legitimate friend trusted by the target (Van Den Bergh & Pretorius, 2017). Phishing attempts, malware attacks, and password attacks are examples of social engineering tools (Rama, 2016; Sarika & Varghese, 2017; Baykara & Gürel, 2018).

2.4.4 Distributed Denial of Services attacks (DDoS)

DDoS attack means causing an online service to be down or unavailable (Gu & Liu, n.d). A malware is then injected into the user's computer so that the user's attention can be drawn to the DDoS attack, which will give the cyber-criminal access into a system (Pandey *et al*., 2016).

2.4.5 Botnets

Botnets are a network of infected computer systems that are controlled by hackers who perform illegal activities such as sending spams (Antonioli, Bernieri, & Tippenhauer, 2018). These illegal activities are performed by making use of computer bots to put together a network of infected computer systems (Pandey *et al*., 2016).

Botnets exploit internet services like Hypertext Transfer Protocol (hereafter, HTTP), Internet Relay Chat (hereafter, IRC), email, and Domain Name System (hereafter, DNS) in order to commit other cybercrimes such as DDoS, malware distribution and identity theft (Antonioli *et al*., 2018).

2.5 IMPACTS OF CYBER RISK INCIDENTS ON THE BANKING INDUSTRY

The impacts of cyber risk incidents are always detrimental (Shackleford, 2015). After a successful cyberattack, businesses may experience monetary penalties, piracy, legal costs, drops in stock price, security costs, loss of customer confidence and overall damage to reputation (Shackleford, 2015; Pandey *et al*., 2016). The banking industry is strongly impacted by cybercrime, and common impacts of cyber risk incidents experienced by banks are financial losses, fraud, reputational damage, impacts on competitiveness, and business interruptions (McLean, 2013; Lagazio *et al*., 2014; Jensen *et al*., 2017; Strauss, 2017). The impacts of cyber risk incidents in the banking industry are further discussed below:

2.5.1 Financial losses

Following a cybercrime incident, a bank is most likely to launch forensic investigations which require time, effort and most importantly, money (Lagazio *et al*., 2014; Strauss, 2017; Zhijun & Ning, 2017; Kopp *et al*., 2017). Other ways in which banks can lose money after a cyberattack are through overspending on remedying the damage caused and indemnifying customers who may have lost money during cybercrime incidents (Lagazio *et al*., 2014; Lemieux, 2015; Cox & Lahti, 2017). Some cyber risk incidents, for example, identity theft and phishing, have a direct impact on the profitability of the affected organisation (Minniti, 2016; Jensen *et al*., 2017).

In addition to cybercrime investigations, impacts on profitability, remedying processes and indemnifying customers, cyberattacks result in massive financial losses simply because cyber-criminals are always financially motivated (Lemieux, 2015; Pandey *et al*., 2016; Strauss, 2017). It is always the main aim of cyber attackers to extort money from the victim, especially from banks (Dzomira, 2014). According to the South African anti phishing report, South African banks have lost considerable amounts of money to phishing attackers (Mbelli & Dwolatzky, 2016). Bank customers also suffer significant financial losses to malware attackers, who use customers' computers, mobile phones and tablets to steal from them (Lemieux, 2015).

2.5.2 Fraud

Advanced cyberattacks such as malware attacks and identity theft result in the perpetration of fraud (Dzomira, 2014). More banking fraud incidents are foreseeable in the future due to ongoing advancements in technology and cybercrime in banking, (Standard Bank, 2017). Banking fraud is committing fraud by making use of online technology to illegally transfer money from one bank account to another (Alese *et al*., 2018). Fraud in banking is an area of concern globally and has negative financial impacts on both banks and bank customers (Dzomira, 2014).

2.5.3 Reputational damage

Reputational damage refers to negative impacts on an organisation's brand and its customer relations (Kopp *et al*., 2017). Customers may suffer financial losses as well as inconvenience when having to replace their bank cards and bank accounts (Shackleford, 2015; Cox & Lahti, 2017). As a result, angry customers may complain on public platforms such as social media, consequently contributing to damaging the bank's reputation (McLean, 2013). Reputational damage can result in revenue losses, diminished customer loyalty, and loss of customers to competitors (Lagazio *et al*., 2014).

2.5.4 Impacts on competitiveness

The banking industry is a heavily competitive industry (Lagazio *et al*., 2014). As soon as customers are affected by cybercrime taking place in their bank, they are most likely to move to the next bank (Strauss, 2017; Lagazio *et al*., 2014)

2.5.5 Business interruptions

Cyberattacks can detrimentally affect a computer systems' normal functioning (Strauss, 2017). This may result in banks experiencing business interruptions (Ben-Asher & Gonzalez, 2015; Deloitte, 2015).

2.6 CYBER RISK MANAGEMENT (CYBERSECURITY)

In the past, banks used to guard themselves against heavily armed burglars who broke into banks in order to physically steal money from till points and vaults (Brady, 2018). However, in this age, crimes against banks are committed in cyberspace because large amounts of money and information are kept there (Dzomira, 2014; Alese *et al*.,

2018). For this reason, it is important for banks in this age to employ effective cybersecurity measures in order to manage cyber risk (Dzomira, 2014; Pricewaterhousecoopers, 2016).

Cybersecurity refers to measures put in place in order to protect information infrastructures and the organisation's network from cyber-criminals (Ben-Asher & Gonzalez, 2015; Van Den Bergh & Pretorius, 2017). Information infrastructures are inclusive of computer systems, telecommunication systems, processes, networks, facilities, technological assets and the internet (Lemieux, 2015; Van Den Bergh & Pretorius, 2017). Cybersecurity is also defined as an approach to safeguard cyberspace from cybercrime, such as information breaches (Mclean, 2013; Mbelli & Dwolatzky, 2016). In essence, it is a holistic approach for managing cyber risk that covers prevention, mitigation and reaction (Mclean, 2013).

2.6.1 The importance of cybersecurity in the banking industry

Cybersecurity is important for banks since the banking industry is the most targeted by cyber-criminals (Shackleford, 2015; Baker, 2015; SARB, 2017). Thus, banks need to decide on cybersecurity methods in order to manage the cyber risks they are exposed to (Kopp *et al*., 2017; Alese *et al*., 2018). These cybersecurity methods should not only be appropriate but should also be commensurate with the cyber risks facing the industry (Kopp *et al*., 2017).

2.6.2 Cybersecurity methods for banks

Banks should always be cognisant of the fact that the nature of cybercrime will continue to evolve, and should therefore ensure that their adopted cybersecurity methods keep pace with evolving cybercrime (Lemieux, 2015; Deloitte, 2018). Common cybersecurity methods include fire walls, encryptions, and keeping backup or archive records at a separate location (Kopp *et al*., 2017). Banks can also transfer risk to a third party by purchasing a cyber insurance policy whereby the insurer will cover losses or damages resulting from cybercrime incidents (Lemieux, 2015; Kopp *et al*., 2017). Cybersecurity awareness and education for bank users and employees is another important cybersecurity method (Dzomira, 2014; Pandey *et al*., 2016; Alese *et al*., 2018). In addition to these methods, it is important for the banking industry to follow a suitable framework in managing cybercrime and ensuring that the cyber risk problem is not compounded (Cassim, 2011). Chapter 3 elaborates on this framework.

2.7 CRITICAL LINK TO THE STUDY

The stated research problem relates to the management of cyber risks in the banking industry. In order to solve the research problem, one of the objectives was to identify and explain cyber risks that the banking industry is exposed to as well as the need for effective cyber risk management methods in the banking industry. Therefore, this chapter discussed the different types of cybercrime prevalent in the banking industry, the causes of cybercrime, the impacts of cybercrime, and the importance of cyber risk management methods in the banking industry.

2.8 CONCLUSION

This chapter discussed cyber risks in banking, their causes and impacts on business. Bank digitisation is the main reason cybercrime has become intense in banking. It was established that since the very early stages of technology, the banking industry has been a primary target for cyber-criminals. As a result, banks suffer numerous and sophisticated cyberattacks, with phishing being the most frequent cyber risk in banking. Inadequate cybercrime laws and lack of appropriate legal frameworks are also notable reasons for this thriving cybercrime. The aim of cyberattacks is usually financial gain. Consequently, banks can suffer massive financial losses, among other things, following a cybercrime incident. Crimes against banks in this age are committed in cyberspace due to the fact that large amounts of money and information are kept there. Thus, it is important that banks should employ effective cybersecurity methods to manage cyber risks. In addition to cybersecurity methods, adhering to a suitable cyber risk management framework for managing risk is important.

The following chapter discusses the risk management framework currently adopted by the South African banking industry, namely BASEL III. The ICIC framework and the CPMI–IOSCO cyber resilience guidance are also studied in depth.

CHAPTER THREE

RISK MANAGEMENT FRAMEWORKS AND THE CPMI–IOSCO CYBER RESILIENCE GUIDANCE

3.1 INTRODUCTION

A number of South African legislations have been passed for the purpose of combating the growth of cybercrime (Mbelli & Dwolatzky, 2016). These include the Electronic Communications and Transmissions Act 25 of 2002, the Electronic Communications Security Pty (Ltd) Act 68 of 2002, and the Protection of Personal Information Act 4 of 2013 (Sutherland, 2017). Despite these Acts, the banking industry is still experiencing increased complexity in combating and managing cybercrime (Barclays, 2017). As a result, the industry has resorted not only to complying with these regulations but also manages cyber risks through frameworks (Svatá & Fleischmann, 2011; Kopp *et al*., 2017).

Cyber risks differ from other risks in nature and sophistication (Internet Security Alliance, 2013; Kopp *et al*., 2017). As a result, a framework designed to manage all risks is not sufficient, nor is it effective in managing cyber risks because of their different nature and high complexity (NIST, 2014). It is therefore important for the banking industry to have a framework in place that specifically addresses the management of cyber risk (Kopp *et al*., 2017).

3.2 RISK MANAGEMENT FRAMEWORKS IN THE BANKING INDUSTRY

A framework currently adopted by the banking industry in South Africa is BASEL (Standard Bank, 2012; Barclays, 2017). BASEL is a regulatory framework designed to strengthen the capital base of the banking industry because a weak capital base can lead to a financial crisis, which will in turn weaken the economy (Gomes, King & Lai, 2017; Boora & Kavita, 2018). Therefore, the key purpose of the BASEL framework is to promote a more secure and resilient financial system, thereby stabilising the banking industry and the economy (Deloitte, 2014).

The global financial crisis that took place in 2008 brought about greater focus on the significance of implementing the BASEL framework (Boora & Kavita, 2018). Following the global financial crisis, there have been frequent additions to the BASEL framework, causing it to become more complex (Deloitte, 2014). Due to this increased complexity,

most banks find it difficult to implement the BASEL framework (Adesina, 2017). According to a study conducted in 2016, South African bankers are of the view that the BASEL framework is irrelevant within the South African banking system, and the implementation thereof will lead to increased banking costs (Nkopane, 2016).

Over the years, BASEL has been developed from BASEL I to BASEL III (Nkopane, 2016). The BASEL III framework consists of three pillars. (Achterberg & Heintz, 2012; Basel Committee on Banking Supervision, 2017). The first pillar provides the capital calculations requirements for credit, market and operational risks (Achterberg & Heintz, 2012). The second pillar outlines the process through which a bank should review its overall capital adequacy (BCBS, 2017). The second pillar also addresses a bank's risk management processes and the supervision thereof (Deloitte, 2014). In the third pillar, the BASEL III framework provides disclosure requirements for the reporting of risks, risk management and capital, with the intention of strengthening market discipline (BCBS, 2017). The challenge with the BASEL III risk management framework is that it is generic to overall risks, thus it is ineffective in managing cyber risk (Svatá & Fleischmann, 2011; Kopp *et al*., 2017). The ICIC framework, on the other hand, is designed to specifically manage cyber risks (NIST, 2014).

The ICIC framework is commended for its flexibility, robustness, cost effectiveness and efficiency in managing cyber risks, hence it is widely adopted by banks across the globe (Spitzner, 2017; Miron & Muita, 2014; Clozel, 2016). The numerous banks that have adopted the ICIC framework have found it to be an effective and helpful cyber risk management tool (Stechyshyn, 2015; Spitzner, 2017; Roman, 2014). It is also important to note the flexibility that the ICIC framework provides to organisations, and the ability to modify it in order to suit those organisations' unique cyber risks, cyber risk tolerance and cyber risk management objectives, thus making it easy to implement (NIST, 2014; Spitzner, 2017). The Financial Stability Institute is of the opinion that the ICIC framework is a valuable starting point for effectively managing cyber risk (Crisanto & Prenio, 2017).

3.3 THE EVOLUTION OF THE ICIC FRAMEWORK

The ICIC framework was issued by NIST (Stechyshyn, 2015). It was developed through a collaboration between the private sector and the U.S.A's government (Stine, Quill, & Witte, 2014). It was designed to secure critical infrastructures against cyber

risks since they are targets for cyberattacks (Benardo & Weatherby, 2015). Critical infrastructure refers to assets and systems, either virtual or physical, which are vital to a country (Ciglic, McKay, Hering & Moore, 2017). The incapacity or destruction of such assets and systems can result in negative impacts on the security, national public health, national economic security and safety of that country (Stine *et al*., 2014). These critical infrastructures include financial systems among other things (Miron & Muita, 2014). The ICIC framework provides procedures for understanding, managing and reporting cyber risk both internally and externally (Stine *et al*., 2014)

The creation of the ICIC framework relied on existing international standards, practices and procedures that have proven to be effective (Roman, 2014). The framework is continually revised as implementation stakeholders discover areas of development (Ciglic *et al*., 2017). The revisions reflect the continually evolving nature of cybercrime (Dimon, Sweet & Bolten, 2018).

There are currently two versions of the ICIC framework (Eggers, 2018). Version 1.0 was issued in February 2014 and version 1.1 was issued in April 2018 (Eggers, 2018; Benardo & Weatherby, 2015). Version 1.1 is not a replacement but rather an update of version 1.0 (Eggers, 2018). It emphasises that businesses should assess their cyber risks, along with the costs and benefits of their cyber risk management strategies (Eggers, 2018).

3.4 OVERVIEW OF THE ICIC FRAMEWORK

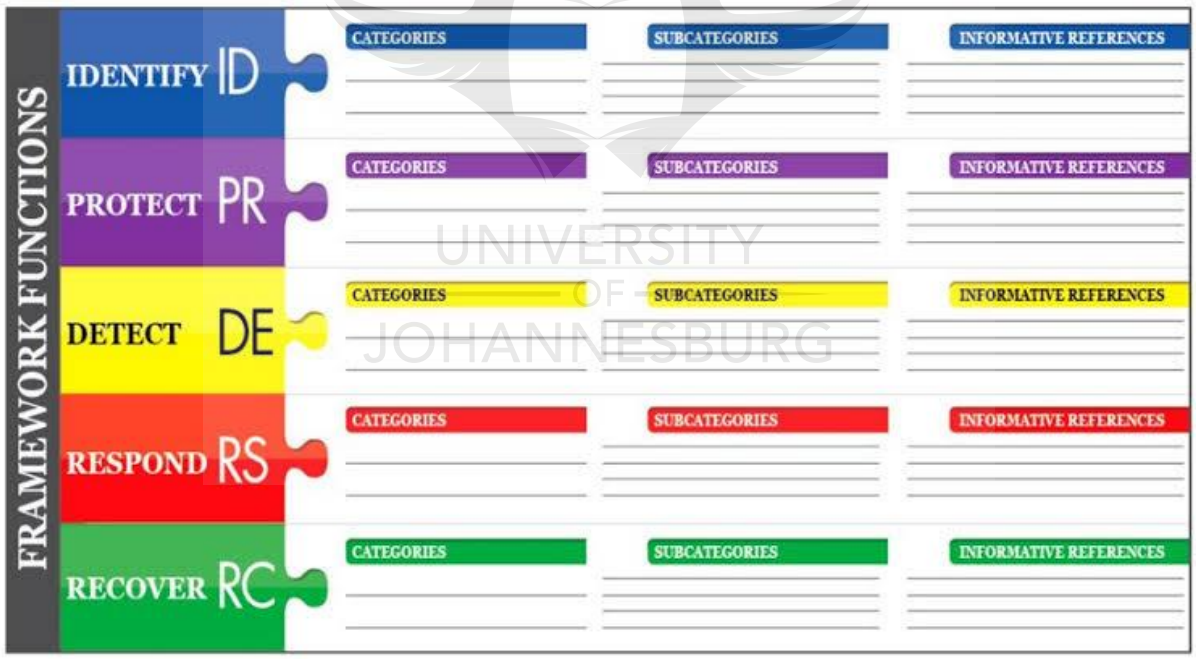
The ICIC framework is risk-based and is made up of three components: the framework core, the framework profile and the implementation tiers (NIST, 2014; Stine *et al*., 2014). These components are further discussed in the following sections.

3.4.1 The framework core

The framework core is a set of cybersecurity activities, their expected outcomes, and relevant references that are common across critical infrastructures (Anderson, 2017). It is made up of five functions, which are presented in the first column of Table 3.1 below (Vigliarolo, 2017). These functions help organisations express their cyber risk management by arranging information, addressing threats, enabling risk management decisions, and are improved by learning from preceding activities (NIST, 2018). Under each function, the framework core identifies fundamental categories and

subcategories as illustrated in Table 3.1 (Stine *et al*., 2014). In the second column named ‘categories’, an organisation should subdivide a function into groups of cybersecurity categories of objectives directly connected to program-related needs and specific activities (NIST, 2018). Examples of these categories are asset management, detection processes, access control, and identity management (Keller, 2018). In the third column labeled ‘subcategories’, an organisation should further divide each category into a set of expected results that will lead to the achievement of the cybersecurity objectives provided in each category (NIST, 2018). Each subcategory is then matched with informative references (Keller, 2018). Informative references, in the fourth column, are the guidelines, standards, practices or methods an organisation elects to implement in order to achieve the results expected from each subcategory (Stine *et al*., 2014). Table 3.1 below is an illustration of the framework's core structure (NIST, 2018).

Table 3.1: Framework core structure



The five framework core functions mentioned above are defined in the following sections.

3.4.1.1 Identify

The activities in this function are fundamental and critical to the effective usage of the framework (NIST, 2018). It is important for organisations to have a complete

understanding of their digital and physical assets and their interconnectedness (Anderson, 2017). Organisations must identify and understand the following (NIST, 2018):

- The business context;
- The resources that support critical functions; and
- The related cybersecurity risks.

Understanding the above will aid the organisation to correctly focus their cyber risk management efforts (Anderson, 2017). Outcome categories within this function include asset management, governance, business environment, risk assessment and risk management strategy (NIST, 2018).

3.4.1.2 Protect

The protect function enables organisations to alleviate the impact of a possible cybercrime incident (NIST, 2014). In this function, organisations must ensure that there are appropriate access controls to safeguard their digital and physical assets (Anderson, 2017). Outcome categories within this function include data security, management and access control, awareness and training, maintenance, protective technology and procedures for information protection (NIST, 2018).

3.4.1.3 Detect

Within this function, organisations must have measures in place to identify cybercrime events in a timely manner (Anderson, 2017). Outcome categories in this function include irregularities and events, detection processes and continuous monitoring (NIST, 2018).

3.4.1.4 Respond

The respond function means taking action to address a detected cybercrime event and minimise the impact thereof (Anderson, 2017). Response planning, communication, analysis mitigation and improvements are the outcome categories that fall within this function (NIST, 2018).

3.4.1.5 Recover

This function supports the ability to restore functions and infrastructures affected by cybercrime incidents (NIST, 2014). Recovering to normal operations as soon as

possible will minimise the impact of cybercrime events (Anderson, 2017). Recovery planning, communication, and improvements are the outcome categories within this function (NIST, 2018).

3.4.2 The framework profile

The framework profile involves the process of aligning the framework's core functions and categories with the organisation's business requirements, resources and risk tolerance (Stine *et al*., 2014). It also helps organisations to describe the state of cybersecurity activities (Keller, 2018). This is done by establishing road maps in order to identify gaps between achieved cybersecurity outcomes and outcomes that still need to be achieved (Vigliarolo, 2017). Finally, action plans to address these gaps need to be developed to make sure that every cybersecurity outcome is achieved (NIST, 2018).

3.4.3 The framework implementation tiers

There are four tiers of implementation (Anderson, 2017). The tiers represent the degrees of rigour and complexity in cyber risk management activities (NIST, 2018). They range from tier one to tier four (Keller, 2018). Tier one is called 'Partial', tier two 'Risk Informed', tier three 'Repeatable' and tier four 'Adaptive' (Vigliarolo, 2017). The higher tiers are considered the more complete implementation of the framework (NIST, 2018). The following section discusses the CPMI–IOSCO cyber resilience guidance, against which the ICIC framework is mapped in Chapter 4.

3.5 CPMI–IOSCO GUIDANCE ON CYBER RESILIENCE FOR FMIs

CPMI–IOSCO cyber resilience guidance for FMIs was issued by CPMI and IOSCO on 29 June 2016 (SARB, 2017; World Federation of Exchanges, 2018). Every South African bank is required by the SARB to align their cyber risk management processes and practices to the CPMI–IOSCO cyber resilience guidance (SARB, 2017; Standard Bank, 2017). The South African Registrar of Banks uses this as a basis to assess the adequacy of the South African banks' cyber risk management processes and practices (SARB, 2017). This guidance is the latest best practice relating to cyber risk management, and is believed to be useful for building or improving cyber risk management frameworks for banks (SIFMA, 2016; SARB, 2017; Deloitte, 2018).

The CPMI–IOSCO cyber resilience guidance provides that a bank should firstly have a cyber risk management framework (European Central Bank, 2016). The guidance contains guidelines that should be addressed within a bank's cyber risk management framework (BIS & IOSCO, 2016). These guidelines are intended to strengthen the effective and consistent supervision and oversight of the banking industry's cyber risk management (Financial Stability Board, 2016; European Central Bank, 2016).

3.5.1 The purpose of the CPMI–IOSCO cyber resilience guidance

Recognising the sophisticated and evolving nature of cybercrime, the CPMI–IOSCO guidance contains guidelines that require evolving methods to address cyber risks (BIS & IOSCO, 2016). The primary purpose of this guidance is to mitigate the evolving risk of cybercrime in banking by providing the industry with guidance to improve their cyber resilience capabilities (Financial Stability Board, 2016). Cyber resilience, for the purposes of this guidance, means the ability of a bank to anticipate, withstand, contain and quickly recover from a cybercrime incident (BIS & IOSCO, 2016; World Bank Group, 2017).

Even though this guidance may be applicable to other industries, it is primarily targeted towards the banking industry (European Central Bank, 2016). CPMI and IOSCO strongly recommend that banks should already have a cyber risk management framework, cyber risk controls, policies and practices in place, as the guidance is not meant to replace them but to enhance those (BIS & IOSCO, 2016). Therefore, this guidance should be considered only as a reference for overseeing and implementing a cyber risk management framework (Financial Stability Board, 2016). Most importantly, the guidelines of this guidance should not be applied in contradiction to applicable laws and regulations (SARB, 2017)

Given the interconnectedness of the banking industry, it is important that all banks utilise this guidance in order to achieve the desired outcomes for cyber resilience (Financial Stability Board, 2016; European Central Bank, 2016; World Federation of Exchanges, 2018). In May 2017, the SARB issued a guidance note, the purpose of which was to bring the attention of all South African banks to the CPMI–IOSCO cyber resilience guidance document (SARB, 2017). The SARB issued this guidance note to ensure that banks were developing cyber resilience capabilities enabling them to quickly recover from cybercrime incidents (Standard Bank, 2017). The CPMI–ISOCO

guidance document is the latest international best practice relating to cyber risk management (SARB, 2017). It is for this reason that the SARB requested banks to align their cyber risk management practices to this cyber resilience guidance (SARB, 2017). In the guidance note, the SARB also mentioned that it would assess the adequacy of the banks' cyber risk management practices, based on the CPMI–IOSCO cyber resilience guidance (SARB, 2017).

3.5.2 The CPMI–IOSCO cyber resilience guidelines

The CPMI–IOSCO guidance outlines eight guidelines made up of five fundamental risk management categories and three overarching categories that should be addressed within any cyber risk management framework for banks (BIS & IOSCO, 2016; SARB, 2017). The fundamental categories include governance, identification, protection, detection, response and recovery, while overarching elements include testing, situational awareness, learning and evolving (World Bank Group, 2017; SARB, 2017). These categories of guidelines were designed to lead cyber resilience strategies, standards and frameworks (European Central Bank, 2016). Below is a discussion of the CPMI– IOSCO guidelines.

3.5.2.1 Governance

Cyber governance refers to procedures implemented by banks to establish, execute and assess their cyber risk management practices (World Federation of Exchanges, 2018). This process should start with a clear and comprehensive cyber risk management framework guided by the bank's cyber resilience strategy and should be aligned to the organisation's operational risk management framework (European Central Bank, 2016). The framework should define how the bank's cyber resilience objectives and cyber risk tolerance will be determined, articulate how the bank will effectively detect, alleviate and manage cyber risks, and outline its people, processes and technology requirements to manage cyber risk (BIS & IOSCO, 2016). Most importantly, the framework should clearly define the board and management's roles and responsibilities relating to cyber risk management (European Central Bank, 2016).

First and foremost, the board's responsibility is to set up the cyber risk management framework, endorse it, and set the bank's cyber risk tolerance (World Federation of Exchanges, 2018). Management, on the other hand, is responsible for overseeing the

implementation of the cyber risk management framework as well the controls, policies and practices that support it (European Central Bank, 2016).

3.5.2.2 Identification

The bank should identify its business functions and processes and perform a risk assessment thereon (World Federation of Exchanges, 2018). The risk assessment will help the bank to thoroughly understand the importance of each function and process, as well as how they are interdependent (BIS & IOSCO, 2016). The bank should then classify identified functions and processes in the order of their criticality (European Central Bank, 2016). This classification will inform the bank's prioritisation of its cyber risk management efforts (BIS & IOSCO, 2016). The bank should repeat the same process for its information assets and system configurations (European Central Bank, 2016). Then the list of identified functions, processes, information assets and system configurations should be regularly reviewed and updated in order to ensure that it remains complete, accurate and current (European Central Bank, 2016). The bank should identify the cyber risks it assumes from and poses to other organisations with which they are interconnected (BIS & IOSCO, 2016). The bank, together with the organisations with which it is interconnected, should collaborate and improve overall cyber resilience capabilities (European Central Bank, 2016).

3.5.2.3 Protection

Even though Information and Communications Technology (hereafter, ICT) is not a focal point of this guidance, it is recommended that banks should build a strong ICT control environment because it is fundamental to cyber risk management (BIS & IOSCO, 2016). For example, the bank should have measures in place such as encryptions, access controls, and ICT system configurations (European Central Bank, 2016).

In addition to a strong ICT control environment, the bank should ensure that from the design stage of a system, it considers cyber resilience by implementing appropriate protective controls (BIS & IOSCO, 2016). Protective controls should be aligned to the bank's cyber risk tolerance (European Central Bank, 2016). It is also important that the bank implements protective measures against insider threats such as previous and even current employees (World Federations of Exchanges, 2018). Banks can achieve this by performing background checks on new employees, regular checks on all

employees throughout their employment, role-based access controls, and staff training on detecting, reporting and addressing cyber risks (BIS & IOSCO, 2016). Further, protective controls against cyber risks posed by organisations with which the bank is interconnected must be implemented (World Federations of Exchanges, 2018).

3.5.2.4 Detection

Banks need to ensure that they continuously monitor and detect cyberattacks in real time through establishing security operations centres (European Central Bank, 2016). Banks should be able to detect both publicly known and unknown cyberattacks, and should establish multi-layered detection controls that cover processes, technology and people (BIS & IOSCO, 2016; European Central Bank, 2016). Lastly, banks should have procedures in place to record and assess detected cyberattacks (BIS & IOSCO, 2016).

3.5.2.5 Response and recovery

After detecting a cyberattack or attempt, a bank should launch an investigation in order to establish the nature and degree of damage caused by the attack (BIS & IOSCO, 2016). During the investigation, the bank should take measures to address the situation in order to avoid more damage and most importantly, resume operations (European Central Bank, 2016). The bank's systems should be designed in a way that the bank is able to safely resume critical functions within two hours of the cyberattack (World Federation of Exchanges, 2018). In addition to the two hours' recovery plan, banks should plan for scenarios where this objective may not be achievable due to the unavailability of critical people, processes, or systems for considerable periods (European Central Bank, 2016).The response, resumption and recovery plans should be tested for effectiveness and should be closely integrated with business continuity management, disaster recovery plans, and crisis management of the bank (World Federation of Exchanges, 2018).

As it is important to maintain data integrity, banks should ensure that their processes and systems are designed and tested to recover accurate data after a cybercrime incident (BIS & IOSCO, 2016). Should data integrity be compromised after a successful cyberattack, banks may have to request uncorrupted data from third parties (European Central Bank, 2016). Therefore, banks should arrange to keep data backed

up with a trusted third party from whom the bank can request data in the event that data integrity is compromised following a cyberattack (BIS & IOSCO, 2016).

3.5.2.6 Situational Awareness

Banks should identify cyber risks that may potentially have a significant impact on their ability to perform business functions and settle obligations (European Central Bank, 2016). Banks should also identify potential cyber risks with the availability, integrity and confidentiality of their business processes and reputation (BIS & IOSCO, 2016). The list of these cyber risks should be analysed, and the analysis regularly reviewed and updated (European Central Bank, 2016). This process will ensure the implementation of cyber resilience measures that are well cyber risk-informed (BIS & IOSCO, 2016).

3.5.2.7 Learning and evolving

Banks should have systems in place to identify lessons learnt from cybercrime occurrences, so they may improve their cyber risk management processes (European Central Bank, 2016). Banks must also keep an update of the latest technologies and new methods of cyber risk management (BIS & IOSCO, 2016). Furthermore, banks should not only be reactive but must also be proactive in order to effectively address future cyber risks (European Central Bank, 2016).

3.5.2.8 Testing

The bank's cyber risk management framework should continuously be tested for effectiveness, and the test results should be used to improve its cyber resilience practices (BIS & IOSCO, 2016; European Central Bank, 2016). Various testing methods include vulnerability assessment, scenario-based testing, penetration tests and red team tests to test the effectiveness of the cyber risk management framework (European Central Bank, 2016).

Vulnerability assessment involves detecting, assessing and remedying security weaknesses in the processes and systems of a bank (BIS & IOSCO, 2016). The bank should conduct a subsequent validation assessment to ensure that security weaknesses have been remedied (BIS & IOSCO, 2016). Scenario-based testing can be conducted by simulating a broad scope of possible scenarios to test the bank's response, resumption, and recovery plans (European Central Bank, 2016). Banks

should also test the ability of their employees and processes to respond to uncommon scenarios of cyberattacks (BIS & IOSCO, 2016).

A penetration test requires that weaknesses that might have an impact on the bank's networks, systems, processes and people should be identified (European Central Bank, 2016). Furthermore, this test should simulate actual cyberattacks on the system to test whether the cyberattack is able to penetrate the system (BIS & IOSCO, 2016). This test should be performed on a regular basis, and each time the systems are updated (European Central Bank, 2016). Red team tests involve setting up red teams, which test the bank's cyber risk controls for effectiveness and possible weaknesses (BIS & IOSCO, 2016). A red team may comprise external experts or the bank's own employees (European Central Bank, 2016). The bank should also participate in industry-wide testing, as this can help the bank to identify weaknesses that may not have been identified in its cyber risk management processes (BIS & IOSCO, 2016).

3.6 CRITICAL LINK TO THE STUDY

Having identified the cyber risks that the banking industry is exposed to and the need for effective cyber risk management methods, the study aimed at discussing cyber risk management frameworks for the South African banking industry and the CPMI–IOSCO cyber resilience guidance. This chapter identified the risk management framework currently adopted by the South African banking industry for managing cyber risk and discussed the ICIC framework and the CPMI–IOSCO cyber resilience guidance.

3.7 CONCLUSION

This chapter identified existing legislations designed to address cybercrime in South Africa. It was established that even though these legislations exist, the banking industry is still confronted with the risk of cybercrime. The South African banking industry manages risks, including cyber risk, through the implementation of the BASEL III framework. However, the BASEL III framework is not specific to the management of cyber risks, and therefore is ineffective in managing them. The chapter further discussed the ICIC framework, which was designed specifically to manage cyber risks, and is widely adopted by banks across the globe. The chapter highlighted the ability of the ICIC framework to be modified to suit any organisation's specific needs and

objectives. This chapter also discussed the CPMI–IOSCO cyber resilience guidance for FMIs, which provides that banks should have a cyber risk management framework that addresses the guidelines contained therein.

In the following chapter, the ICIC framework practices are mapped against the CPMI–IOSCO cyber resilience guidelines. The results of the mapping are analysed and discussed.

CHAPTER FOUR

THE EMPIRICAL STUDY AND RESEARCH FINDINGS

4.1 INTRODUCTION

The literature review presented in Chapters 2 and 3 identified the cyber risks facing the banking industry. It also highlighted that this industry is the most vulnerable to cybercrime (Grobler, 2018). This is evidenced by the increased number of cyberattacks in the banking industry compared to other industries (Lagazio *et al*., 2014). As a result, it is important for banks to ensure effective management of cyber risks (Shackleford, 2015). Effective cyber risk management ensures that potential cyberattacks do not occur, and that the impact of their occurrence is avoided or lessened (Wong & Shi, 2015).

In the literature review, it was noted that South African banks are required by the SARB to align their cyber risk management processes to the CPMI–IOSCO cyber resilience guidance, which contains guidelines that should be addressed within a bank's cyber risk management framework (BIS & IOSCO, 2016; SARB, 2017). The literature also identified BASEL III, a risk management framework currently adopted by the South African banking industry (Standard Bank, 2012). It was established in the literature review that the BASEL III framework is ineffective in managing cyber risks (Kopp *et al*., 2017). However, the ICIC framework is an effective, flexible and helpful framework for managing cyber risks (Roman, 2014). It is for this reason that the ICIC framework is widely adopted by a considerable number of banks internationally (Stechyshyn, 2015).

In this chapter the researcher analyses the ICIC framework, in order to map it against the CPMI–IOSCO cyber resilience guidelines. The research findings will be evaluated in order to establish whether the ICIC framework addresses the guidelines as set out in the CPMI–IOSCO cyber resilience guidance

4.2 MAPPING OF THE ICIC FRAMEWORK AGAINST THE CPMI–IOSCO CYBER RESILIENCE GUIDELINES

The CPMI–IOSCO cyber resilience guidelines are made up of five fundamental risk management categories and three overarching categories, as discussed in Chapter 3 (SARB, 2017). Table 4.1 and 4.2 below present the categories in the first column. The

second column outlines the guidelines provided in each category. This information was extracted from the CPMI–IOSCO cyber resilience guidance document issued in 2016. The mapping takes place in the last column. The mapping was done by replying 'YES' or 'NO' next to each CPMI–IOSCO guideline in the last column. 'YES' indicates that there is an ICIC framework practice that matches the CPMI–IOSCO guideline. 'NO' indicates that the CPMI–IOSCO guideline is not addressed by the ICIC framework. An explanation of the outcome is also discussed. The ICIC framework practices are gathered through an analysis of the latest version 1.1 of the ICIC framework, which refines, clarifies and improves the preceding version (NIST, 2018).

4.2.1 CPMI–IOSCO guidelines – fundamental risk management categories

Table 4.1 presents the mapping of the ICIC framework against the CPMI–IOSCO cyber resilience guidelines provided under the fundamental risk management categories.

Table 4.1: CPMI–IOSCO Guidelines – Fundamental risk management categories mapping

FUNDAMENTAL RISK MANAGEMENT CATEGORIES (CPMI–IOSCO CYBER RESILIENCE GUIDANCE)	GUIDELINES (CPMI–IOSCO CYBER RESILIENCE GUIDANCE)	ICIC FRAMEWORK PRACTICES
1. Governance	1.1. The board should set up a cyber risk management framework, endorse it and set the bank's cyber risk tolerance.	**YES** When the bank adopts the ICIC framework, they would not need to set up a new framework. The ICIC framework stipulates that the bank should determine the level of cyber risk they consider acceptable, and this level should be expressed as a cyber risk

		tolerance. This risk tolerance should be displayed in the selected implementation tier. Implementation tiers are discussed in section 3.4.3.
	1.2. Management should oversee the implementation of the cyber risk management framework and the controls, policies and practices that support it.	**YES** As per the ICIC framework, management should approve and communicate the performance of the framework activities and ensure that framework activities are properly performed.
	1.3. The framework should define how the bank's cyber risk tolerance will be determined.	**YES** The bank's cyber risk tolerance determination should be informed by the bank's role in the country's critical infrastructure and industry risk assessment.
	1.4. The framework should define how the bank's cyber resilience objectives will be determined.	**NO** The ICIC framework does not define how cyber resilience objectives will be determined. It only defines how to determine cyber resilience objectives that are not yet achieved.
	1.5. The framework should articulate how the bank will	**YES** The ICIC framework core consists of functions that

	effectively detect, alleviate and manage cyber risks.	are intended to detect, alleviate and manage cyber risks.
	1.6. The framework should outline its people and processes to manage cyber risk.	**YES** As per the ICIC framework, an organisation should identify and understand cyber risk management systems, processes and people. The processes are outlined in the framework core and the people should include the executive management level staff, the business/process level staff and the implementation/ operation level staff.
	1.7. The framework should outline technology requirements to manage cyber risk.	**NO** The ICIC framework does not outline technology requirements to manage cyber risk.
	1.8. The framework should clearly define the board's roles and responsibilities relating to cyber risk management.	**NO** The role and responsibilities of the board regarding cyber risk management are not defined in the ICIC framework.
	1.9. The framework should clearly define management's roles and responsibilities	**YES** The roles and responsibilities of management are clearly

	relating to cyber risk management.	defined in the ICIC framework. Their role is to communicate and monitor the implementation of the framework activities.
2. Identification	2.1. Identify the bank's business functions, processes, information assets and system configurations.	**YES** This framework requires that the organisation should identify and understand its business context, critical functions, systems, its information and physical assets.
	2.2. Perform a risk assessment on the items identified in 2.1.	**YES** In the 'identify' function of the ICIC framework, an organisation is required to perform risk assessment on the business, its critical functions, systems, information and physical assets.
	2.3. Classify the items in 2.1 in the order of their criticality.	**YES** The items identified above should be classified in the order of their criticality and business value so that they can be prioritised accordingly.
	2.4. The list generated in 2.3 should be regularly reviewed and updated.	**NO** The framework does not mention that there should be a regular review and

		update of the list of the items above.
	2.5. Identify cyber risks the bank assumes from and poses to other organisations with which they are interconnected.	**NO** The ICIC framework recognises that some cyber risks are assumed and posed to other organisations with which they are interconnected. However, it does not require that an organisation should specify where the identified cyber risk is assumed from or posed to.
3. Protection	3.1. Banks should build a strong ICT control environment (e.g. encryptions, access controls, and ICT system configurations).	**YES** An organisation should set up appropriate safeguards, such as access control, protective technology and data security.
	3.2. From the design stage of a system, the bank should implement appropriate protective controls aligned to the bank's cyber risk tolerance.	**YES** Implementation of safeguards should be based on the set cyber risk tolerance.
	3.3. Implement protective measures against insider threats, such as previous and even current employees of the bank.	**YES** Safeguards should be implemented against both internal and external threats.
	3.4. Implement protective controls against cyber risks	**YES**

	posed by the organisations with which the bank is interconnected.	Even though an organisation is not required to specify that some identified cyber risks are posed by an organisation with which they are interconnected, safeguards should be implemented against all cyber risks identified.
4. Detection	4.1. Continuously monitor and detect cyberattacks in real time by setting up a security operations center.	**NO** The ICIC framework provides that an organisation should establish detection processes and continuously monitor cybercrime events. However, it does not require that the monitoring and detection of cybercrime events be done in real time.
	4.2. Detect both publicly known and unknown cyberattacks.	**YES** The ICIC frameworks requires that all cyberattacks should be detected, whether publicly known or unknown.
	4.3. Establish multi-layered detection controls that cover processes, technology and people.	**YES** Detection controls include monitoring the physical environment, personnel activities, external service

		provider activities, devices, software and systems for possible cybercrime events.
	4.4. Record and assess detected cyberattacks.	**YES** An organisation should keep a record of detected and identified cyberattacks in order to assess how they are managed.
5. Response and recovery	5.1. After detecting a cyberattack or attempt, a bank should launch an investigation in order to establish the nature and degree of damage caused by the attack.	**YES** Following a cyberattack, an organisation should analyse the impact thereof.
	5.2. Take measures to address the situation in order to avoid more damage.	**YES** Measures that should be taken after detecting a cyberattack are, analyse the impact, implement measures to minimise that impact, improve protective measures that were penetrated by the cyber-criminal, and recovery to normal operations.
	5.3. Design the bank's system in a way that the bank is able to resume operations within at least two hours of the cyberattack.	**NO** This framework does not provide the time within which to resume operations after a cyberattack.

		However, it emphasises that resumption to normal operations should take place as soon as possible.
	5.4. Plan for scenarios where resuming within two hours may not be achievable due to unavailability of critical people, processes, or systems for considerable periods.	**NO** This framework does not provide the time within which to resume operations after a cyberattack. However, it emphasises that resumption to normal operations should take place as soon as possible.
	5.5. The response, resumption and recovery plans should be tested for effectiveness.	**YES** Tests and analysis of response and recovery activities should be conducted to ensure they are effective.
	5.6. The response, resumption and recovery plans should be closely integrated with business continuity management, disaster recovery plans and crisis management of the bank.	**YES** An organisation's response plans should be in line with business continuity plans. Recovery plans should be in line with disaster recovery plans.
	5.7. Ensure that processes and systems are designed and tested to recover accurate data after a cybercrime incident.	**YES** Backups of data must be conducted, maintained and tested to ensure recovery of data following a cybercrime incident.

4.2.2 CPMI–IOSCO guidelines – overarching categories

Table 4.2 presents the mapping of the ICIC frameworks against the CPMI–IOSCO cyber resilience guidelines provided under the overarching categories.

Table 4.2: CPMI–IOSCO Guidelines – Overarching categories mapping

OVERARCHING CATEGORIES (CPMI – IOSCO CYBER RESILIENCE GUIDANCE)	GUIDELINES (CPMI–IOSCO CYBER RESILIENCE GUIDANCE)	ICIC FRAMEWORK PRACTICES
6. Testing	6.1. Continuously test the bank's cyber risk management framework for effectiveness.	**NO** This framework does not address the subject of framework testing.
	6.2. Use the test results to improve the cyber resilience practices. Various testing methods include vulnerability assessment, scenario-based testing, penetration tests and red team tests. These testing methods are discussed in section 3.5.2.8.	**NO** This framework does not address the subject of framework testing.
7. Situational awareness	7.1. Identity cyber risks that may potentially have significant impact on the bank's ability to perform business functions and settle its obligations.	**YES** The ICIC framework requires that for each cyber risk identified, an analysis, including impact analysis, should be conducted thereon.
	7.2. Identify cyber risks that may have a potential impact	**YES**

	on the availability, integrity and confidentiality of business processes.	The ICIC framework requires that for each cyber risk identified, an analysis, including impact analysis, should be conducted thereon.
	7.3. Identify cyber risks that may have a potential impact on the bank's reputation.	**YES** The ICIC framework requires that for each cyber risk identified, an analysis, including impact analysis, should be conducted thereon.
	7.4. The list of these cyber risks should be analysed, and the analysis should be regularly reviewed and updated.	**NO** According to the ICIC framework, all cyber risks should be analysed. However, it is not specified anywhere in the ICIC framework that they should be regularly reviewed and updated.
8. Learning and evolving	8.1. Have systems in place to identify lessons learnt from cybercrime occurrences.	**YES** Response plans should incorporate identifying and documenting lessons learned from detected cyberattacks.
	8.2. Use the lessons identified to improve the cyber risk management processes.	**YES** Organisational response activities and cybersecurity activities should be improved by incorporating

		lessons learned from cyberattack detection and response activities.
	8.3. Keep an update of the latest technologies and new methods of cyber risk management.	**YES** An organisation needs to actively adapt to evolving technology and cybersecurity methods in order to effectively manage this ever-evolving cybercrime.

The analysis of the results from the mapping conducted in Table 4.1 and 4.2 above are presented and discussed in the following section.

4.3 RESEARCH FINDINGS: THE CPMI–IOSCO CYBER RESILIENCE GUIDELINES ADDRESSED BY THE ICIC FRAMEWORK

The aim of this research is to establish whether the ICIC framework addresses the guidelines as set out in the CPMI–IOSCO cyber resilience guidance. The mapping in Table 4.1 and 4.2 was conducted in order to determine the degree to which the ICIC framework addresses the CPMI–IOSCO cyber resilience guidelines. Figure 4.1 below presents the analysis of the results from the mapping.

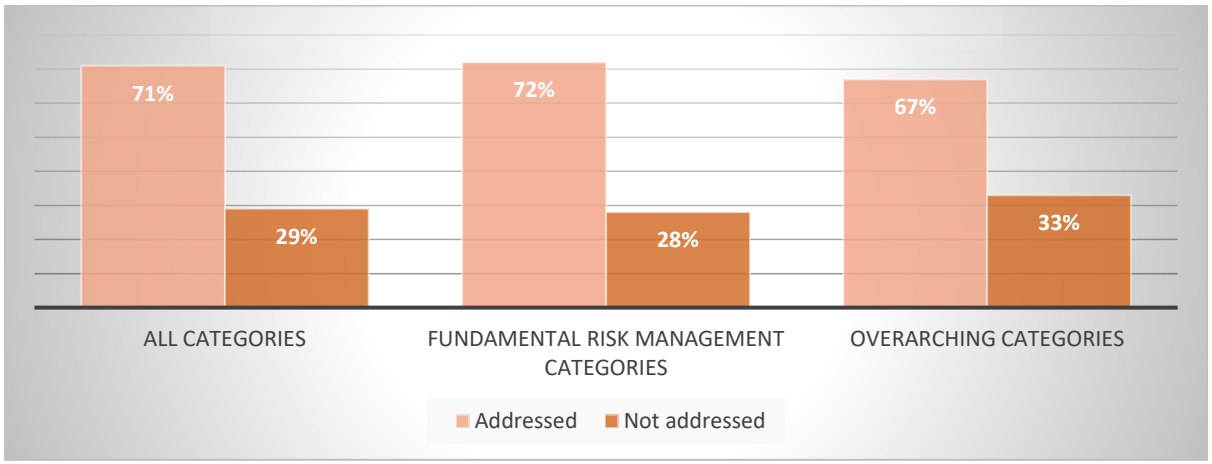


Figure 4.1: An analysis of the mapping of the ICIC framework against the CPMI–IOSCO guidelines

The results from the mapping reveal that the degree to which the ICIC framework addresses all the CPMI–IOSCO cyber resilience guidelines is 71 percent. The CPMI–IOSCO cyber resilience guidelines not addressed by the ICIC framework are mostly made up of guidelines provided under the overarching categories. The 33 percent of guidelines not addressed under the overarching categories are mainly represented by the 'testing' category. This is because the ICIC framework does not address 'framework testing'. Only 28 percent of the guidelines provided under the fundamental risk management categories are not addressed by the ICIC framework. The 28 percent is predominantly represented by the guidelines provided under the 'governance' category, owing to the fact that the same categories of guidelines under fundamental risk management, except 'governance', make up the ICIC framework core discussed in section 3.4.1.

4.4 RECOMMENDED CYBER RISK MANAGEMENT FRAMEWORK

According to the SARB guidance note issued to South African banks in 2017, South African banks must align their cyber risk management processes to the CPMI–IOSCO cyber resilience guidance (Standard Bank, 2017). The guidance requires that banks should have a cyber risk management framework in place. This cyber risk management framework must address the guidelines contained in the CPMI–IOSCO cyber resilience guidance. The ICIC framework addresses up to 71 percent of these guidelines.

It was established that as a result of the ICIC framework being flexible, an organisation can modify it to meet its specific needs and objectives. Therefore, the study recommends that, instead of building a new cyber risk management framework, South African banks should adopt the ICIC framework, as it already significantly addresses the CPMI–IOSCO guidelines. South African banks can then modify it by adding only 29 percent of the CPMI–IOSCO guidelines not addressed by the ICIC framework. In that manner, all the CPMI–IOSCO guidelines will be addressed by the modified version of the ICIC framework. The researcher recommends the ICIC framework to the South African banking industry for the following reasons:

- Unlike the BASEL framework, it is not generic to overall risks, but is specific to cyber risk management;
- It already addresses a considerable number of the CPMI–IOSCO guidelines;

- It has been adopted by numerous banks across the globe;
- It has proven to be effective for managing cyber risks;
- It is efficient, cost effective and easy to implement; and
- It is flexible.

South African banks should modify the ICIC framework by adding the following features to it (BIS & IOSCO, 2016):

- The way in which the bank's cyber resilience objectives will be established should be defined in the framework.
- In the framework, the bank should define all the technology they require to manage cyber risk.
- The framework should clearly describe the roles and responsibilities of the board and management regarding cyber risk management.
- The list of identified business functions, information assets, system configurations and processes should be regularly reviewed and updated.
- Identify the cyber risks that the bank is exposed to as a result of its interconnection with other organisations.
- Identify the cyber risks that the bank poses to other organisations with which they are interconnected.
- The bank's systems must be designed in a manner that allows for operations to resume within at least two hours after a cyberattack.
- Plan for cases whereby resuming within two hours may not be possible because of unavailable critical people, processes, or systems for considerable periods.
- The list of cyber risks threatening the bank's reputation, ability to perform business functions, and the availability, integrity and confidentiality of business processes, should be analysed and the analysis should be regularly reviewed and updated.
- The bank's cyber risk management framework (in this case, the ICIC framework) must be continuously tested for effectiveness.
- The test results must be used to develop and enhance cyber risk management practices.

4.5 CRITICAL LINK TO THE STUDY

The main objective of the study was to recommend to the South African banking industry, a cyber risk management framework that is effective and that addresses the guidelines contained in the CPMI–IOSCO cyber resilience guidance. This chapter mapped the ICIC framework to the CPMI–IOSCO cyber resilience guidelines in order to establish the extent to which the ICIC framework addresses the guidelines as set out in the CPMI–IOSCO cyber resilience guidance. This chapter also recommended the ICIC framework to the South African banking industry.

4.6 CONCLUSION

This chapter reflected on the aim of the study, which is to establish whether the ICIC framework addresses the guidelines as set out in the CPMI–IOSCO cyber resilience guidance. The aim of the study was achieved by mapping the ICIC framework to the CPMI–IOSCO guidelines. This was conducted in order to test the degree to which the ICIC framework addresses the CPMI–IOSCO guidelines. The mapping results revealed that 71 percent of the CPMI–IOSCO guidelines are addressed by the ICIC framework. The researcher recommended that South African banks adopt the ICIC framework and modify it by adding to it the 29 percent of the CPMI–IOSCO guidelines not addressed by the ICIC framework. By so doing, all the CPMI–IOSCO guidelines will addressed by the modified ICIC framework. Moreover, the ICIC framework is effective, efficient, flexible, cost effective and easy to implement.

The following chapter summarises the results deduced from the literature review and the empirical study. Thereafter, conclusions are drawn and areas for future research suggested.

CHAPTER FIVE

CONCLUSIONS

5.1 INTRODUCTION

This chapter presents a summary of the results deduced from the literature review in chapter 2 and 3. This chapter will also highlight the results of the empirical study presented in chapter 4. Finally, this chapter will suggest possible areas for future research.

5.2 DEDUCTIONS

The literature review in Chapter 2 and 3 indicated that due to technological advancements, the banking industry is experiencing greater efficiency and effectiveness in business. At the same time, threats such as cyber risk have surfaced as a result of these technological advancements. The banking industry is the most attacked industry by cyber-criminals, thus banks should implement effective cyber risk management processes. The literature review also indicated that cyber risk management processes implemented by South African banks should be aligned to the CPMI–IOSCO cyber resilience guidance. The CPMI–IOSCO cyber resilience guidance provides that banks should have a cyber risk management framework and that this framework must address the guidelines contained in the CPMI–IOSCO cyber resilience guidance. Finally, the literature review discussed the ICIC framework. It was established that the ICIC framework is effective, efficient, flexible, cost effective and easy to implement. Chapter 4 mapped the ICIC framework against the CPMI–IOSCO cyber resilience guidelines in order to establish the degree to which the ICIC framework addresses the CPMI–IOSCO cyber resilience guidelines. The following sections summarise the results from the literature review and the empirical study.

5.2.1 Literature review

The results deduced from the literature review are as follows:

- The banking industry has experienced the most cybercrime incidents compared to other industries.
- The nature of cybercrime in banking will continue to evolve.
- With the continuous growth in technology, cybercrime incidents have become numerous and sophisticated.

- In addition to IT and advancements in technology, other causes of cybercrime include global connectivity, the internet, and the digitisation of banks.
- The risk of cybercrime in African countries including South Africa, is magnified by the lack of IT skills and appropriate legal frameworks at national level.
- A common range of cybercrimes include identity theft, malware, social engineering, DDoS, and botnets.
- A phishing attack, which is one of the types of malware, is the most frequent cybercrime in South African banks.
- According to security experts, 91 percent of all cybercrimes start with a phishing attack.
- One of the most extreme cybercrimes is ransomware, which is another type of malware where the cyber-criminal locks user access to files and systems and then demands a ransom to unlock user access.
- Cybercrime incidents have detrimental impacts on the banking industry, for example, financial losses, fraud, reputational damage, impacts on competitiveness and business interruptions.
- Given the detrimental impacts that cybercrime has on the banking industry, and the industry being the most targeted by cyber-criminals, it is vital for banks to employ effective cyber risk management processes.
- Cyber risk management processes employed by banks should keep pace with the evolving nature of cybercrime.
- Banks should adopt a framework that is designed specifically to manage cyber risk, because a framework designed to manage an organisation's overall risk is not sufficient to manage cyber risks.
- BASEL III, a framework adopted by the South African banking industry, is not sufficient for managing cyber risk because it is generic to overall risks.
- The ICIC framework was designed to specifically manage cyber risks.
- The ICIC framework is effective for managing cyber risk, efficient, cost effective and easy to implement.
- The ICIC framework is flexible, hence an organisation can modify it to meet its specific needs and objectives.
- The ICIC framework is widely adopted by banks across the globe and has been found to be useful and effective.

- South African banks are required by the SARB to align their cyber risk management process to the CPMI–IOSCO cyber resilience guidance document.
- The South African Registrar of Banks will use the CPMI–IOSCO cyber resilience guidance document as a basis to assess the adequacy of the South African banks' cyber risk management processes.
- The CPMI–IOSCO cyber resilience guidance provides that banks must have a cyber risk management framework that addresses the guidelines contained in the CPMI–IOSCO cyber resilience guidance.

5.2.2 The empirical study and research findings

The results deduced from the empirical study are as follows:

- The ICIC framework addresses up to 71 percent of the guidelines contained in the CPMI–IOSCO cyber resilience guidance document.
- Only 28 percent of the CPMI–IOSCO cyber resilience guidelines under the fundamental risk management categories are not addressed by the ICIC framework.
- The remaining 28 percent of the CPMI–IOSCO cyber resilience guidelines under the fundamental risk management categories not addressed by the ICIC framework, is mostly represented by the 'governance' guidelines.
- 67 percent of CPMI–IOSCO cyber resilience guidelines provided under the overarching categories are addressed by the ICIC framework.
- The 33 percent of the guidelines provided under the overarching categories not addressed by the ICIC framework is due to the fact that the ICIC framework does not address 'framework testing'.

5.3 POSSIBLE AREAS FOR FUTURE RESEARCH

This study recommends the ICIC framework to the South African banking industry. The framework is recommended because with the implementation of this framework, South African banks will achieve effective cyber risk management and the framework will address all the CPMI–IOSCO guidelines after it is modified. The SARB announced this request through a guidance note issued in May 2017. The following possible area for future research is suggested:

- An investigation of cyber risk management measures or frameworks adopted by South African banks following the guidance note issued by the SARB and establish if they address the CPMI–IOSCO cyber resilience guidelines.
- Exploring other frameworks to establish the extension to which they address the CPMI–IOSCO cyber resilience guidelines, in order to consider a hybrid framework.
- Mapping the BASEL III framework against the CPMI–IOSCO cyber resilience guidance to determine how far it addresses the CPMI–IOSCO cyber resilience guidelines.

5.4 CONCLUSION

This chapter presented a summary of the results deduced from the literature review, and the research findings from the empirical study. The study investigated cybercrimes that the banking industry is faced with. It was found that in South Africa, phishing attacks are the most frequent cybercrime. It was highlighted that it is important for the banking industry to implement effective cyber risk management processes, as it is the industry most targeted by cyber-criminals. As required by the SARB, South African banks should align their cyber risk management processes to the CPMI–IOSCO cyber resilience guidance, which provides that banks should have a cyber risk management framework. This cyber risk management framework should address the guidelines contained in the CPMI–IOSCO cyber resilience guidance. The main aim of the study was to establish whether the ICIC guidelines contained in the CPMI–IOSCO cyber resilience guidance are addressed within the ICIC framework. The research findings revealed that the ICIC framework addresses up to 71 percent of the CPMI–IOSCO cyber resilience guidelines. Having established that, the researcher recommended that South African banks should adopt the ICIC framework and modify it by adding the 29 percent of the CPMI–IOSCO cyber resilience guidelines not addressed by the ICIC framework. The researcher recommends the ICIC framework because it already addresses the CPMI–IOSCO cyber resilience guidelines significantly, and after modification it will address all of them. Moreover, the ICIC framework is effective, flexible, cost-effective and easy to implement.

REFERENCE LIST

Achterberg, E. & Heintz, H. (2012). *Basel III Summary*. Available from: https://www.nist.gov/cyberframework/online-learning/five-functions (Accessed on 28 July 2018).

Adesina, K. S. (2017). *Essays on Basel III capital requirements and its effects in the African banking sector*. (Thesis). Auckland Park, Johannesburg: University of Johannesburg. Available from: http://hdl.handle.net/10210/262435 (Accessed on 13 November 2018).

Agrawal, S. (2016). Cyber Crime in Banking Sector. *Udgam Vigyati – The origin of knowledge*, 3:1-19. Available from: http://www.udgamvigyati.org/admin/images/Cyber%20Crime%20in%20Banking%20Sector-%20Sanchi%20Agrawal.PDF (Accessed on 27 April 2018).

Alese, B. K., Thompson, A. F., Alowolodu, O. D. & Oladele, B. (2018). Multilevel authentication system for stemming crime in online banking. *Interdisciplinary Journal of Information, Knowledge and Management*, 13: 79-94. doi: http://0-dx.doi.org.ujlink.uj.ac.za/10.28945/4063. Available from: http://0-go.Galegroup.com.ujlink.uj.ac.za/ps/i.do?p=AONE&u=rau_itw&id=GALE|A544712903&v=2.1&it=r&sid=ebsco (Accessed on 10 July 2018).

Anderson, E. (2017). *How to comply with the 5 functions of the NIST cybersecurity framework*. Available from: https://www.secmatters.com/blog/how-to-comply-with-the-5-functions-of-the-nist-cybersecurity-framework (Accessed on 29 September 2018).

Antonioli, D., Bernieri, G. & Tippenhauer, N. O. (2018). *Taking control: Design and implementation.of botnets for cyber-physical attacks with CPSBot*. Available from: http://arxiv.org/abs/1802.00152 (Accessed on 28 June 2018).

Asgary, A. (2016, June). *Business Continuity and Disaster Risk Management in Education: Case of York University.* Available from: http://0-edsa.ebscohost.com.ujlink.uj.ac.za/eds/pdfviewer/pdfviewer?vid=1&sid=d6aeef79-cbb6-4008-a6e1-4649705cf2fb%40sessionmgr4009 (Accessed on 5 July 2017).

Ashford, W. (2016, November). Tesco Bank cyber attack prompts security warning from Financial Conduct Authority. *Computer Weekly*. Available from: http://0-search.ebscohost.com.wam.city.ac.uk/login.aspx?direct=true&db=bth&AN=119484764&site=ehost-live (Accessed on 21 April 2018).

Baker, C. (2015). Over-regulation and cyber risk top CEOs' list of threats to banking and capital markets growth. *Credit Control*, 36 (1): 6-7. Available from: http://0-eds.a.ebscohost.com.ujlink.uj.ac.za/eds/detail/detail?vid=0&sid=5500b925-2e32-43e6-8b2b-0146324aec4b%40sessionmgr4009&bdata=JnNpdGU9ZWRzLWxpdmUmc2NvcGU9c2l0ZQ%3d%3d#AN=110644993&db=f5h (Accessed on 10 July 2018).

Bank for International Settlements & International Organization of Securities & Commissions. (2016). *Guidance on cyber resilience for financial markets*

infrastructures. Available from: https://www.bis.org/cpmi/publ/d146.pdf (Accessed on 28 July 2018).

Barclays. (2017, June). *Barclays Africa Group Limited 2017 Integrated Report*. Available from: https://www.barclaysafrica.com/content/dam/barclays-africa/bagl/pdf/results/annual/2017-integrated-report.pdf (Accessed on 18 June 2018).

Basel Committee on Banking Supervision. (2017). *Basel III: Finalising post-crisis reforms*. Available from: http://www.bis.org/bcbspubl/d424.htm (Accessed on 30 July 2018).

Baykara, M. & Gürel, Z. Z. (2018). Detection of phishing attacks. *IEEE Xplore*, doi: 10.1109/ISDFS.2018.8355389. Available from: https://0-ieeexplore-ieee-orgujlink.uj.ac.za/document/8355389/?arnumber=8355389&SID=EBSCO:edseee (Accessed on 27 June 2018).

Ben-Asher, N. & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *SciVerce Science Direct,* 48: 51-61. Available from: https://doi.org/10.1016/j.chb.2015.01.039 (Accessed on 10 July 2018).

Benardo, M. B. & Weatherby, K. M. (2015). A framework for cybersecurity. *Supervisory Insights*. Available from: https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin15/si_winter2015-article01.pdf (Accessed on 20 September 2018).

Bengtsson, M. (2016). How to plan and perform a qualitative study using content analysis. *Elsevier*, 2: 8-14. Available from: https://doi.org/10.1016/j.npls.2016.01.001 (Accessed on 13 September 2018).

Berisha-Shaqiri, A. (2015, March). Impact of Information Technology and Internet in Businesses. *Academic Journal of Business, Administration, Law and Social Sciences*, 1(1): 2410-3918. Available from: http://iipccl.org/wp-content/uploads/2015/03/Ajbals-73-79.pdf (Accessed on 06 March 2018).

Bevan, O., Ganguly, S., Kaminski, P. & Rezek, C. (2016). *The ghost in the machine: Managing technology risk.* Available from: https://www.mckinsey.com/~/media/McKinsey/Business Functions/Risk/Our Insights/The ghost in the machine managing technology risk/The-ghost-in-the-machine-Managing-technology-risk.ashx (Accessed on 06 April 2018).

Binuyo, A. O. & Aregbeshola, R. A. (2014, March). The impact of information and communication technology (ICT) on commercial bank performance: evidence from South Africa. *Problems and Perspectives in Management*, 12(3): 59-68. Available from: https://www.researchgate.net/publication/268979895_The_impact_of_information_and_communication_technology_ICT_on_commercial_bank_performance_Evidence_from_South_Africa (Accessed on 03 March 2018)

Bishnoi, T.R & Devi, S. (2017). Information technology in banking system. In *Palgrave Macmillan Studies in Banking and Financial Institutions*. Palgrave Macmillan: n.p.

Available from: https://www.palgrave.com/gp/series/14678 (Accessed on 05 March 2018).

Boora, K. K. & Kavita, J. (2018). Implementation of Basel III Norms in Banking Industry: A Review of Empirical Literature. *The IUP Journal of Bank Management*, 17 (3): 7-24. Available from: http://content.ebscohost.com/ContentServer.asp?EbscoContent=dGJyMNLr40Sep7E4zOX0OLCmr1CeprVSsaa4SrKWxWXS&ContentCustomer=dGJyMPGssVGup7VRuePfgeyx9Yvf5ucA&T=P&P=AN&S=R&D=bth&K=131613195 (Accessed on 13 November 2018).

Brady, S. (2018). *Banks lead the fight against cyber risk*. Available from: http://0-eds.b.ebscohost.com.ujlink.uj.ac.za/eds/pdfviewer/pdfviewer?vid=1&sid=502f4671-6596-4ec3-9a6e-17d0b575c17a%40sessionmgr101 (Accessed on 27 June 2018).

Camillo, M. (2016). Cybersecurity: Risks and management of risks for global banks and financial institution. *Journal of Risk Management in Financial Institutions*, 10 (2): 196-200. Available from: https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/Insights/jrmfi-mark-camillo-article-mar-2017.pdf (Accessed on 23 April 2018).

Cassim, F. (2011). Addressing the growing spectre of cyber crime in Africa: evaluating measures adopted by South Africa and other regional role players. *The Comparative and International Law Journal of Southern Africa*, 44 (1): 123-138. Available from: https://0-www-jstor-org.ujlink.uj.ac.za/stable/23253117 (Accessed on 28 June 2018).

Ciglic, K., McKay, A., Hering, J. & Moore, T. (2017). *Cybersecurity policy framework. A practical guide to the development of national cybersecurity policy*. Available from: https://www.microsoft.com/en-us/cybersecurity/content-hub/Cybersecurity-Policy-Framework (Accessed on 28 August 2018).

Clozel, L. (2016). Banks Get (Yet Another) Cybersecurity Framework, This Time from G-7. *American Banker*. Available from: https://www.Americanbanker.com/news/banks-get-yet-another-cybersecurity-framework-this-time-from-g-7 (Accessed on 20 September 2018).

Cox, R. Q. C & Lahti, L. (2017). Cyber-attacks on banks: the consequences of a loss of access to bank records. *Butterworths Journal of International Banking and Financial Law:* 127–129. Available from: http://www.quadrantchambers.com/images/uploads/documents/spotlight_-_News.pdf (Accessed on 10 July 2018).

Crisanto, J. C. & Prenio, J. (2017). *FSI insights on policy implementation No 2. Regulatory approaches to enhance banks' cyber-security frameworks*. Available from: https://www.bis.org/fsi/publ/insights2.pdf (Accessed on 20 September 2018).

Dandago, K. I. & Rufai, A. S. (2014). Information technology and accounting information system in the Nigerian banking industry. *Asian Economic and Financial Review*, 4(5): 655-670. Available from: http://www.aessweb.com/journals/5002 (Accessed on 27 July 2018).

Deloitte. (2014). *Basel III framework. The butterfly effect*. Available from: https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/financial-services/sea-fsi-basel-III-framework-noexp.pdf (Accessed on 28 July 2018).

Deloitte. (2015). Deloitte financial reporting conference. *Rising to the challenge*. Available from: https://www2.deloitte.com/content/dam/Deloitteie/Documents/Audit/ie_2015_FRC_Limerick_Deloitte_Ireland.pdf (Accessed on 13 June 2018).

Deloitte. (2016). *Information technology risks in financial services: What board members need to know – and do*. Available from: https://www2.deloitte.com/za/en/pages/risk/articles/information-technology-risks-financial-services.html (Accessed on 06 March 2018).

Deloitte. (2018). *Cyber risk and regulation in Europe. A new paradigm for banks*. Available from: https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Risk/IE_FS_Cyber_risk_regulation_0218_draft32.pdf (Accessed on 20 June 2018).

Dimon, J., Sweet, J. & Bolten, J. (2018). *Comments on cybersecurity framework version 1.1 draft 2*. Available from: https://www.nist.gov/sites/default/files/documents/2018/01/31/2018-01-19_-_business_roundtable.pdf (Accessed on 28 August 2018).

Dzomira, S. (2014). Electronic fraud (cyber fraud) risk in the banking industry, Zimbabwe. *Risk Governance & Control: Financial Markets & Institutions*, 4(2): 17-27. Available from: https://doaj.org/article/1d7c01313790408b9735408e4d2f43d6 (Accessed on 28 June 2018).

Eggers, M. J. (2018). *One and Done? Not for NIST and the Cyber Framework*. Available from: https://www.uschamber.com/series/above-the-fold/one-and-done-not-nist-and-the-cyber-framework (Accessed on 28 August 2018).

Elo, S. & Kyngäs, H. (2007). The qualitative content analysis process. *Journal of Advanced Nursing*, 62 (1): 107-115. Available from: https://student.cc.uoc.gr/uploadFiles/192-%CE%A3%CE%A0%CE%95%CE%9D407/CONTENT%20ANALYSIS.pdf (Accessed on 13 September 2018)

Ernst & Young. (2017, June). *Petya cyber attack. EY responses to the global cybersecurity incident*. Available from: https://www.ey.com/Publication/vwLUAssets/ey-petya-cyber-attack/ $FILE/ey-petya-cyber-attack.pdf (Accessed on 10 July 2018)

Eruemegbe, G.O. (2015, April). Effect of Information and Communication Technology on Organization Performance in the Banking Sector. *International Journal of Research in Engineering and Technology*, 3(4): 13-22. Available from: editor@impactjournals.us (Accessed on 03 March 2018).

European Central Bank. (2016). *Cyber resilience oversight expectations (CROE) for financial markets infrastructures*. Available from: https://www.ecb.europa.eu/paym

/pdf/cons/cyberresilience/cyber_resilience_oversight_expectations_for_FMIs.pdf (Accessed on 30 July 2018).

Financial Stability Board. (2016). *Guidance on cyber resilience for financial market infrastructures*. Available from: http://www.fsb.org/2016/06/guidance-on-cyber-resilience-for-financial-market-infrastructures/ (Accessed on 07 August 2018).

First Rand Bank. (2017, June). Annual report for the year ended 30 June 2017. Available from: https://www.firstrand.co.za/InvestorCentre/Current%20FRB%20annual%20report/FirstRand%20Bank%20Limited%20annual%20report%20-%20June%202017.pdf (Accessed on 18 June 2018).

Flinders, K. (2017, August). How banking IT has transformed since the financial crisis. *Computerweekly.com.* Available from: http://0-eds.a.ebscohost.com.ujlink.uj.ac.za/eds/pdfviewer/pdfviewer?vid=1&sid=9ffc0ed6-1c06-479b-b457-26dfb104901c%40sessionmgr4008 (Accessed on 02 March 2018).

Gallegos-Segovia, P. L., Bravo-Torres, J. F., Larios-Rosillo, V. M., Vintimilla-Tapia, P. E., Yuquilima-Albarado, I. F. & Jara-Saltos, J. D. (2017). Social engineering as an attack vector for ransomware. *IEEE Xplore*, doi: 10.1109/CHILECON.2017.8229528. Available from: https://0-ieeexplore-ieee-org.ujlink.uj.ac.za/stamp/stampjsp? tp=& arnumber=8229528 (Accessed on 27 June 2018).

Giahi, R., Sahebjamnia, N. & Torabi, S.A. (2016). An enhanced risk assessment framework for business continuity management systems. *Safety Science*, 86 (2016): 201-218. Available from: http://0-ac.elscdn.com.ujlink.uj.ac.za/ S0925753516301266/1-s2.0-S0925753516301266-main.pdf?_tid=237c384c-615f-11e7-9563-00000aacb361&acdnat=1499244870_5f5785d90f23c6e4ffc9ec1cba9466da (Accessed on 5 July 2017).

Gomes, T., King, S. & Lai, A. (2017). *Shoring up the foundations for a more resilient banking system: The development of Basel III*. Available from: http://content.ebscohost.com/ContentServer.asp?EbscoContent=dGJyMNLr40Sep7E4zOX0OLCmr1CeprdSsK64TbGWxWXS&ContentCustomer=dGJyMPGssVGup7VRuePfgeyx9Yvf5ucA&T=P&P=AN&S=R&D=bth&K=128187434 (Accessed on 13 November 2018).

Grant Thornton. (2017, May). *Ransomware attack 'WannaCry'*. Available from: https://www.grantthornton.ie/globalassets/1.-member-firms/ireland/insights/fact sheets/grant-thornton---ransom-attack.pdf (Accessed on 28 June 2018).

Grobler, J. (2018). Cyber risk from a chief risk officer perspective. *Journal of Risk Management in Financial Institutions*, 11 (2): 125-131. Available from: http://0-eds.b.ebscohost.com.ujlink.uj.ac.za/eds/pdfviewer/pdfviewer?vid=1&sid=49aa4125-3fb9-4d45-90da-3f2f0a478b9a%40pdc-v-sessmgr01 (Accessed on 27 June 2018).

Gu, Q. & Liu, P. (n.d). *Denial of service attack*. Available from: https://s2.ist.psu.edu/ist451/DDoS-Chap-Gu-June-07.pdf (Accessed on 28 June 2018).

Gupta, S.K. & Chavana, S. (2013). Role of Information Technology in Banking Industry. *Global Journal of Enterprise Information System*, 5(1): 19-23. Available from: com.ujlink.uj.ac.za/eds/pdfviewer/pdfviewer?vid=1&sid=523a1f58-1dcc-4cc8-http://0-eds.a.ebscohostaf4c-892d0020ce79%40sessionmgr4007 (Accessed on 27 February 2018).

Harguem, S. & Echatti, H. (n.d). *IT Governance Status in the Tunisian Banking Sector*. Available from: http://0-eds.a.ebscohost.com.ujlink.uj.ac.za/eds/pdfviewer/pdfviewer?vid=1&sid=e0c7a18b-8776-49d9-84ad-5c8b4c463f4b%40sessionmgr4009 (Accessed on 02 March 2018).

Hopkin, P. (2017). *Fundamentals of risk management. Understanding, evaluating and implementing effective risk management*. New York: The Institute of Risk Management. Available from: https://books.google.co.za/books?hl=en&lr=&id=zfvTDQAAQBAJ&oi=fnd&pg=PR5&dq=effective+risk+management&ots=d7HXcvo0oR&sig=BiaBQ8OtnV5-LWMDoSPE67mbU#v=onepage&q=effective%20risk%20management&f=false (Accessed on 03 April 2018).

Internet Security Alliance. (2013). *Sophisticated management of cyber risk*. Available from: http://isalliance.org/publications/2013-05-28_ISA-AIG_White_Paper-Sophisticated_Management_of_Cyber_Risk.pdf (Accessed on 18 September 2018).

Jensen, M. L., Dinger, M., Wright, R. T. & Thatcher, J. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems*, 34 (2): 597-626. Available from: http://0-eds.b.ebscohost.com.ujlink.uj.ac.za/eds/pdfviewer/pdfviewer?vid=1&sid=eda44d72-9a0a-4bfc-84d7-e564752bf945%40pdc-v-sessmgr01 (Accessed on 27 June 2018).

Joo, J. W., Moon, S. Y., Singh, S. & Park, J. H. (2017). S-detector: an enhanced security model for detecting smishing attack for mobile computing. *Springer Science*, 66 (1): 29-38, doi: 10.1007/s11235-016-0269-9. Available from: https://link.springer.com/article/10.1007/s11235-016-0269-9 (Accessed on 10 July 2018).

Keller, N. (2018). *An introduction to the components of the framework*. Available from: https://www.nist.gov/cyberframework/online-learning/five-functions (Accessed on 29 September 2018).

Kgosana, R. (2018). Cybercrime costs SA almost R2.2bn a year. *The Citizen*. Available from: https://citizen.co.za/news/south-africa/crime/2047717/cybercrime-costs-sa-almost-r2-2bn-a-year/ (Accessed on 24 April 2019)

Klopper, H. (2008). The qualitative research proposal. *Curationis*, 31 (4): 62-72. Available from: https://curationis.org.za/index.php/curationis/article/view/1062 (Accessed on 13 September 2018).

Kopp, E., Kaffenberger, L. & Wilson, C. (2017). *Cyber risk, market failures and financial stability*. IMF Working Paper. Available from: https:// www.imf. org/en/ Publications/WP/Issues/2017/08/07/Cyber-Risk-Market-Faiures-and-Financial-Stabili ty-45104 (Accessed on 01 August 2018).

Korte, J. (2017, July). Mitigating cyber risks through information sharing. *Journal of Payments Strategy and Systems*, 11 (3): 203-214. Available from: http://0-eds.b.ebscohost.com.ujlink.uj.ac.za/eds/detail/detail?vid=0&sid=6343f227-1f8d-4c93-8716-7fdfa76f3d43%40sessionmgr102&bdataJnNpdGU9ZWRzLWxpdmUmc2NvcGU9c2l0ZQ%3d%3d#AN=126901332&db=bth (Accessed on 30 April 2018).

Kothari, C.R. (2004). *Research methodology. Methods and techniques.* New Delhi: New Age International Publishers. Available from: http://www.modares.ac.ir/ uploads/Agr.Oth.Lib.17.pdf. (Accessed on 23 September 2017).

Kundu, S., Islam, K. A., Jui, T. T., Rafi, S., Hossain, A. & Chowdhury, I. H. (2018). *Cyber crime trends in Bangladesh, an analysis and ways out to combat the threat*. International Conference on Advanced Communications Technology. Doi: 10.23919/ICACT.2018.8323800. Available from: https://0-ieeexplore-ieee-org.ujlink.uj.ac.za/stamp/stamp.jsp?tp=&arnumber=8323800 (Accessed on 27 June 2018).

Lagazio, M., Sherif, N. & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. *SciVerce Science Direct,* 45: 58-74. Available from: https://doi.org/10.1016/j.cose.2014.05.006 (Accessed on 10 July 2018).

Lata, P. (2016). Role of Information Technology in Banking Sector. *Journal of Commerce and Management Thought,* 7(1): 186-195. Available from: http://0-eds.a.ebscohost.com.ujlink.uj.ac.za/eds/pdfviewer/pdfviewer?vid=2&sid=d09ae76e-57fc-4bc4-bdf4-a780182c7ba3%40sessionmgr4007 (Accessed in 27 February 2018).

Lemieux, M. (2015). Cyber crime, governance and liabilities in the banking and payment industries. *Banking and Finance Law Review*, 31 (1): 113-140. Available from: http://0-resolver.ebscohost.com.ujlink.uj.ac.za/openurl?sid= EBSCO%3alpb&genre=article&issn=08328722&ISBN=&volume=31&issue=1&date=20151101&spage=113&pages=113-140&title=Banking+&atitle=Cyber+Crime%2c+Governance+and+Liabilities+in+the+Banking+and+Payment+Industries.&aulast=Lemieux%2c+Marc&id=DOI%3a&site=ftf-live (Accessed on 28 June 2018).

Li, J. X. (2017). Cyber crime and legal countermeasures: A historical analysis. *International Journal of Criminal Justice Service*, 12 (2): 196-207. doi: 10.5281/zenodo.1034658. Available from: http://0eds.b.ebscohost.com.ujlink.uj.ac.za/eds/detail/detail?vid=0&sid=14b76acb-5f52-41d988a7e72bf9b45860%40sessionmgr104&bdata=JnNpdGU9ZWRzLWxpdmUmc2NvcGU9c2l0ZQ%3d%3d#AN=126901320&db=sih (Accessed on 27 June 2018).

Marinč, M. (2013, February). Banks and information technology: marketability vs. relationships. *Electron Commer Res.*, 13: 71-101. Available from: http://0-eds.b.ebscohost.com.ujlink.uj.ac.za/eds/detail/detail?vid=0&sid=3e3de854-5a70-4255-85af-e958dc035d88%40sessionmgr120&bdata=JnNpdGU9ZWRzLWxpdmUmc2NvcGU9c2l0ZQ%3d%3d#AN=85631836&db=bth (Accessed on 30 April 2018).

Marx, B. & Hohls-du Preez, C. (2017). A risk management disclosure in the integrated reports of the top 40 listed companies on the JSE Limited. *Risk governance and control: financial markets and institutions,* 7(3): 27-34. Available from: http://dx.doi.org/10.22495/rgcv7i3p3 (Accessed on 03 April 2018).

Marx, B., Schönfeldt, N., Van der Watt, A., Van Dyk, V., Maré, D. & Ramuedzisi, T. (2011). *Fundamentals of Auditing*. Johannesburg: LexisNexis.

Maryam, S., Khamesi, S. & Houshang, A. (2016). The impact of cloud-based information technology in improving organizational performance in the banking industry. *International Journal of Advanced Biotechnology and Research*, 7: 388-399. Available from: https://doaj.org/article/4808f81f5f2a4ba5bdf57829ac30f00a (Accessed on 27 February 2018).

Mawudor, B. G., Kim, M. & Park, M. (2015). *Continuous monitoring methods as a mechanism for detection and mitigation of growing threats in banking security systems.* 2015, 4th International Conference on Interactive Digital Media (ICIDM). Available from: http://0-eds.a.ebscohost.com.ujlink.uj.ac.za/eds/detail/detail?vid=0&sid=c4b3de49-3745-4335-9a0b-6bf93fcb348a%40sessionmgr4006&bdata=JnNpdGU9ZWRzLWxpdmUmc2NvcGU9c2l0ZQ%3d%3d#AN=edseee.7516317&db=edseee (Accessed on 23 April 2018).

Mbelli, T. M. & Dwolatzky, B. (2016). *Cyber security, a threat to cyber banking in South Africa*. IEEE Third International Conference on Cyber security and Cloud computing, doi: 10.1109/CSCloud.2016.18. Available from: https://0-ieeexplore-ieee-org.ujlink.uj.ac.za/document/7545887/?arnumber=7545887&SID=EBSCO:edseee (Accessed on 28 June 2018).

McLean, S. (2013). Beware the botnets: Cyber security is a board level issue. *Intellectual Property and Technological Law Journal*, 25 (12). Available from: http://0-content.ebscohost.com.ujlink.uj.ac.za/ContentServer.asp?T=P&P=AN&K=92546232&S=R&D=bth&EbscoContent=dGJyMNLe80SeqLY4yOvsOLCmr1CeprdSsqa4S7aWxWXS&ContentCustomer=dGJyMPGssVGup7VRuePfgeyx43zx (Accessed on 28 June 2018).

Minniti, R. (2016). *Identifying business risk factors of identity theft*. Doctoral dissertation. Washington: Walden University. Available from: https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?referer=https://www.google.co.za/&httpsredir=1&article=4038&context=dissertations (Accessed on 28 June 2018).

Miron, W. & Muita, K. (2014). Cybersecurity capability maturity models for providers of critical infrastructure. *Technology Innovation Management Review*, 4 (10): 33-39. Available from: https://timreview.ca/sites/default/files/article_PDF/MironMuita_TIMReview_October2014.pdf (Accessed on 09 August 2018).

Miyake, K. (2016). Risk management and cyber risk in the financial services sector: an overview. In *Managing cyber risk in the financial sector* (pp. 1-9). Edited by R. Taplin. Available from: https://www.taylorfrancis.com/books/e/9781317383666 (Accessed on 30 April 2018).

Mohurle, S & Patil, M. (2017). A brief study of wannacry threat: Ransomware attack. *International Journal of Advanced Research in Computer Science*, 8 (5): 1938- 1940. Available from: http://www.ijarcs.info/index.php/Ijarcs/article/download/4021 /3642 (Accessed on 28 June 2018)

Nedbank. (2017, December). Nedbank Group Limited Integrated Report. Available from: https://www.nedbank.co.za/content/dam/nedbank/siteassets/AboutUs/Information%20Hub/Integrated%20Report/2017/2017%20Nedbank%20Group%20Integrated%20Report.pdf (Accessed on 18 June 2018).

Nkopane, T. (2016). *The relevance of the BASEL III Accord within the South African banking system*. (Thesis). Johannesburg: University of the Witwatersrand. Available from: https://hdl.handle.net/10539/23804 (Accessed on 14 November 2018).

O'Leary, Z. (2004) *The essential guide to doing research*. New Delhi: Sage Publishers. Available from: https://eunacal.org/metodakerkimi/wp-content/uploads/spss/The_essential_guide_to_doing_research.pdf (Accessed on 13 September 2018).

Page, S. L., Jourdan, G., Bochmann, G. V., Flood, J. & Onut, I (2018). Using URL shorteners to compare phishing and malware attacks. *IEEE Xplore*, doi: 10.1109/ECRIME.2018.8376215. Available from: https://0-ieeexplore-ieee-org.ujlink.uj.ac.za/stamp/stamp.jsp?tp=&arnumber=8376215 (Accessed on 27 June 2018).

Pandey, S., Shah, N., Sharma, A. & Farik, M. (2016). Cybersecurity situation in Fiji. *International Journal of Scientific and Technology Research*, 5 (7): 215-219. Available from: http://www.ijstr.org/final-print/july2016/Cybersecurity-Situation-In-Fiji.pdf (Accessed on 28 June 2018).

Park, D. (2014). *Analysis on mobile forensic of smishing hacking attack*. The Korea Institute of Information and Communication Engineering. International Conference on Future Information and Communication Engineering, 6 (1): 535-538. Available from:

http://www.dbpia.co.kr/Journal/ArticleDetail/NODE07221671 (Accessed on 10 July 2018).

PricewaterhouseCoopers. (2016, March). *Growing in turbulent times. Major banks analysis – South Africa*. Available from: https://www.pwc.co.za/en/assets/pdf/major-banks-analysis-march-2016.pdf (Accessed on 10 July 2018).

Rama, P. (2016). *An evaluation of information technology security threats: A case of the University of Johannesburg*. (Mini Dissertation). Auckland Park, Johannesburg: University of Johannesburg. Available from: http://hdl.handle.net/10210/237303. (Accessed on 4 July 2017).

Rao, M. K. & Yalamanchili, S. (2012). Novel shoulder-surfing resistant authentication schemes using text-graphical passwords. *International Journal of Information and Network Security*, 1 (3): 163-170. Available from: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.921.7720&rep=rep1&type=pdf (Accessed on 13 July 2018).

Roman, J. (2014). *NIST Releases Cybersecurity Framework*. Bank Info Security. Available from: https://www.bankinfosecurity.com/nist-releases-cybersecurity-framework-a-6497 (Accessed on 26 September 2018).

Sahu, P. K. (2013). *Research Methodology: A guide for researchers in Agricultural Science, Social Science and other related fields*. West Bengal: Springer. Available from: https://0-link-springer-com.ujlink.uj.ac.za/content/pdf/10.1007%2F978-81-322-1020-7.pdf (Accessed on 13 September 2018).

Sarika, S. & Varghese, P. (2017). Parallel phishing attack recognition using software agents. *Journal of Intelligent and Fuzzy Systems*, 32: 3273-3284, doi: 10.3233/JIFS-169270. Available from: http://0-eds.b.ebscohost.com.ujlink.uj.ac.za/eds/pdfviewer/pdfviewer?vid=1&sid=65c0edbf-2ca2-45fa-8db8-0ffb1ed685c5%40sessionmgr103 (Accessed on 27 June 2018).

Sattar, S. (2014 09 June). Role of IT in banking sector. *The Nation*. Available from: https://nation.com.pk/09-Jun-2014/role-of-it-in-banking-sector (Accessed on 06 March 2018).

Securities Industry & Financial Markets Association. (2016, February). *CPMI-IOSCO Consultative Report: Guidance on Cyber Resilience for Financial Market Infrastructures*. Available from: https://www.sifma.org/wp-content/uploads/2017 /05/ sifma-submits-comments-to-cpmi-and-iosco-on-their-report-regarding-guidance-on-cyber-resilience-for-financial-market-infrastructures-fmis.pdf (Accessed on 18 June 2018).

Shackleford, D. (2015). Combatting cyber risks in the supply chain. *SANS institute*. Available from: https://www.raytheon.com/capabilities/rtnwcm/groups/cyber/documents/content/rtn273005.pdf (Accessed on 27 June 2018).

Shahriar, H., Klintic, T & Clincy, V. (2015). Mobile phishing attacks and mitigation techniques. *Journal of International Security*, 6: 206-212. Available from: https://file.scirp.org/pdf/JIS_2015063015392117.pdf (Accessed on 10 July 2018).

Shalaginov, A., Johnsen, J. W. & Franke, K. (2017). *Cyber crime investigations in the era of big data*. IEEE International conference on big data: 3672-3676, doi: 10.1109/BigData.2017.8258362. Available from: https://0-ieeexplore-ieee-g.ujlink.uj.ac.za/stamp/stamp.jsp?tp=&arnumber=8258362 (Accessed on 27 June 2018).

Smith, C. (2018). Cybercrime now 55% of gross losses in SA banking industry – report. *Fin24*. Available from: https://www.fin24.com/Companies/Financial-Services/cybercrime-now-55-of-gross-losses-in-sa-banking-industry-report-20181004 (Accessed on 24 April 2019)

South African Reserve Bank, from the office of the Registrar of Banks. (2017). *Guidance Note G4/2017*. Available from: https://www.resban.co.za/Lists/News%20and%20Publications/Attachments/7803/G4%20of%202017.pdf (Accessed on 07 April 2018).

Spitzner, L. (2017, December). *Feedback on NIST CSF – Identify Function – Page 12 line 320*. Available from: https://www.nist.gov/sites/default/files/documents/2018/01/24/2017-12-16-sans.pdf (Accessed on 18 June 2018).

Sravanthi, G. (2016, September). Management of risk issues in E-banking – A case study. *International Journal of Recent Research Aspects*, 3 (3): 38-44. Available from: http://0-eds.b.ebscohost.com.ujlink.uj.ac.za/eds/detail/detail?vid=0&sid=d0369ceb-e730-4eac-8c0a-7b1b96c4e699%40sessionmgr120&bdata=JnNpdGU9ZWRzLWxpdmUmc2NvcGU9c2l0ZQ%3d%3d#AN=119193650&db=a9h (Accessed on 30 April 2018).

Standard Bank. (2012, May). *Basel III – Enhancements to the capital management framework*. Available from: https://thevault.exchange/?get_group_doc=18/1428492110-RMB-MS-Basel-III-Capital-and-Liquidity-event-2-May-2012.pdf (Accessed on 28 July 2018).

Standard Bank. (2017, December). *Standard Bank Group Risk and Capital Management Report 2017.* Available from: http://annualreport2017.standardbank.com/downloads/Standard_bank_AIR2017_standard_bank_group_risk_and_capital_management_report_2017.pdf (Accessed on 18 June 2018).

States News Service. (March 2018). *The banking supervision department clarifies the requirements regarding cyber risk management vis-à-vis the banks' external suppliers*. Available from: http://link.galegroup.com/apps/doc/A543352275/AONE?u=rau_itw&sid=AONE&xid=2982a606 (Accessed 27 June 2018).

Stechyshyn, A. (2015). *Security vulnerability in financial institutions.* Thesis. Utica College. Available from: https://search.proquest.com/docview/1677223944?pq-origsite=gscholar (Accessed on 30 April 2018).

Strauss, P. (2017, September). *Cyber Threats and Responses in the Banking Sector*. CSIR Conference. Available from: https://conference2017.csir.co.za/sites/default/files/Documents/Cyber%20Threats%20and%20Responses%20in%20the%20banking%20sector.pdf (Accessed on 26 July 2018).

Stine, K., Quill, K. & Witte, G. (2014). Framework for Improving Critical Infrastructure Cybersecurity. *ITL Bulletin*. Available from: https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=915476 (Accessed on 09 August 2018).

Sutherland, E. (2017). Governance of cybersecurity – the case of South Africa. *The African Journal of Information and Communication*, 20: 83-112. Available from: https://doi.org/10.23962/10539/23574 (Accessed on 06 August 2018).

Svatá, V. & Fleischmann, M. (2011). IS/IT Risk Management in Banking Industry. *Acta Oeconomica Pragensia*, 19 (3): 42-60. Available from: https://www.vse.cz/polek/download.php?jnl=aop&pdf=334.pd (Accessed on 05 April 2018).

Tiwari, R. & Kumar, R. (2012, September). Information Technology in banking sector. *Asia Pacific Journal of Marketing and Management Review*, 1(1): 25-33. Available from: http://indianresearchjournals.com/pdf/APJMMR/2012/September/ 3.pdf (Accessed on 03 March 2018).

United Nations Office on Drugs & Crime (2013). *Comprehensive study on cybercrime*. New York. Available from: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJEG.4_2013/CYBERCRIME_STUDY_210213.pdf (Accessed on 27 April 2018).

U.S. National Institute of Standards & Technology. (2014). *Framework for Improving Critical Infrastructure Cybersecurity. Version 1.0*. Available from: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf (Accessed on 11 June 2018).

U. S. National Institute of Standards & Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity.* Version 1.1. Available from: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (Accessed on 09 August 2018).

Van Den Bergh, M. & Pretorius, E. (2017). *Cybercitizenship awareness module targeting University of Johannesburg students*. Available from: https://ujcontent.uj.ac.za/vital/access/manager/Repository/uj:24789?queryType=vitalDismax&query=cybersecurity (Accessed on 19 June 2018).

Vigliarolo, B. (2017). NIST cybersecurity framework: A cheat sheet for professionals. *Tech Republic*. Available from: https://www.techrepublic.com/article/nist-cybersecurity-framework-the-smart-persons-guide/ (Accessed on 29 September 2018).

Wong, W. & Shi, W. (2015). Fundamentals of business continuity management. In *Business Continuity Management Systems: A Complete Guide to Implementing ISO22301*. (pp.5-26). Available from: https://0-search-proquest-com.ujlink.uj.ac.za/docview/1809045436/fulltextPDF/D0F2B47045FB440FPQ/1?accountid=13425 (Accessed on 04 April 2018).

World Bank Group. (2017). *Financial sector's cybersecurity: A regulatory digest*. Available from: http://pubdocs.worldbank.org/en/524901513362019919/FinSAC-CybersecDigestOct-2017-Dec2017.pdf (Accessed on 23 April 2018).

World Federation of Exchanges. (2018). *WFE Response to the ECB: Cyber resilience oversight expectations (CROE)*. Available from: www.world-exchanges.org (Accessed on 09 August 2018).

Yadurvedi, N. (2015, October). Emerging Trends in Banking – Increasing Role of Information Technology – Commerce Keywords. *Indian Journal of Applied Research*, 5(10): 636-639. Available from: https://www.researchgate.net/publication/320413997_Emerging_Trends_in_Banking-Increasing_Role_of_Information_Technology_Commerce_Keywords (Accessed on 03 March 2018).

Yeboa-Boateng, E. O. & Amanor, P. M. (2014). Phishing. Smishing & vishing: An assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences*, 5 (4): 297-307. Available from: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.682.2634&rep=rep1&type=pdf (Accessed on 10 July 2018).

Zaeem, R. N., Manoharan, M., Yang, Y. & Barber, K. S. (2017). Modeling and analysis of identity threat behaviors through text mining of identity theft stories. *SciVerce Science Direct,* 65: 50-63. Available from: https://doi.org/10.1016/j.cose.2016.11.002 (Accessed on 27 June 2018).

Zhijun, L. & Ning, W. (2017). *A cyber crime investigation model based on case characteristics*. Fourth International Conference on Information Science and Control Engineering, doi: 10.1109/ICISCE.2017.12. Available from: https://0-ieeexplore-ieee-org.ujlink.uj.ac.za/stamp/stamp.jsp?tp=&arnumber=8110178 (Accessed on 27 June 2018).