A comparison of cyber risk disclosure in the banking sector between South Africa and China

FJ Duvenhage

orcid.org 0000-0003-4283-0603

Mini-dissertation accepted in partial fulfilment of the requirements for the degree *Master of Business Administration* at the North-West University

Supervisor: Prof AM Smit

Graduation: December 2020

Student number: 21158185

MBA 874

Frans Duvenhage

A comparison of cyber risk disclosure in the banking sector between South Africa and China

Abstract

This study is focused on analysing and comparing the practices of cyber risk disclosure within the banking sector of South Africa and China. It evaluates the requirements in both countries and highlights the importance of risk disclosure, and specifically cyber risk disclosure, in the banking sector. The information for this study was obtained by means of document analysis from the 2018 annual reports published by the individual banks. A checklist was developed as a measuring instrument to evaluate the disclosure practices. The results showed a distinct difference between the levels of disclosure of each country, specifically with regards to cyber risk. Further, results also indicate that the type of reports published by South African banks are of a higher quality when compared to those of the banks in China.

Key words: banking sector, South Africa, China, reporting, cyber risk, integrated reporting, the International Financial Reporting Standards (IFRS), disclosure index.

Contents

Chapter 1

Introduction and background

1.1 Introduction to the study

All Stock Exchange listed organisations have to publish their annual financial results (Khlif, Ahmed, Souissi & Sargsyan, 2018). The financial disclosures are more regulated than some of the non-financial disclosures. Due to the fact that the non-financials are not as regulated, organisations struggle to navigate the sometimes confusing landscape of disclosure where numerous frameworks and standards exists (Elshandidy, Shrives, Bamber & Abraham, 2018:2; Krzus, 2011).

To support quality disclosure of information, various reporting guidelines and frameworks have been developed. Previous studies indicate that because financial reporting has been more regulated it is therefore more standardised.

Technological developments over the past 40 years made it easier to do international trade and investment and any business that wants to invest internationally must do due diligence. Annual financial statements are the starting point for any organisation to communicate financial information to the various stakeholders. Proper analysis and investigation requires more than just annual financial results, and the focus has moved to provide additional non-financial information in the report.

When it comes to reporting on non-financial information, the reporting landscape becomes more blurry and unregulated (Stubbs, 2018:503). As the disclosures on risks fall outside of the financial disclosure ambit into the non-regulated side, this study attempts to investigate and compare the risk disclosure of South African and Chinese organisations in the banking sector. After a discussion on risk disclosures in general, the focus of the study will be on the disclosure of cyber risk.

Risk is of vital importance to any organisation and it is a necessity that businesses identify, evaluate, manage and report all types of risk to better external decision-making (CIMA, 2008). Risk is one of the main causes of uncertainty in any organisation and can originate from various sources, both internal and external (Epstein & Rejc, 2006:8). Risk management can be associated with two types of events (Ata & Schmandt, 2016:7):

- Risks, or negative events, and

- Opportunities or positive events.

All investors want principal risk reporting that is specific to an organisation, they want improved disclosure that avoids boilerplate text and which provides enough detail to understand how the organisation accounts for its transactions, how it identified its principle risks and how the organisation is planning to manage those risks (Financial Reporting Council (FRC), 2017:3). Management is able to greatly improve investor confidence when they can prove how the reported risks relate to the business model (FRC, 2017).

The traditional reporting practice is to divide risk management into departments, and each department acts as a silo, reporting and managing only on the specific risk relevant to that department. To illustrate this, the information technology department will handle security risks and the finance department will manage credit, interest and liquidity risks (Ata & Schmandt, 2016:11). As a result, none of the departments are aware of any potential risk or opportunities that could arise from other departments. The 2007 global financial crisis was partially due to the majority of the banks lacking the ability to combine their risk exposures and identify risk concentrations at a bank group level (Thun, 2015).

Each bank identifies a number of key risks to be mitigated to ensure successful operations. Throughout the financial sector more banks are starting to identify cyber risk as a priority risk (Härle, Havas, Kremer, Rona & Samandari, 2016:4). As technology and digital banking has developed in the past decade, cyber risk and the need for reporting on it has emerged as a large player.

To provide more background on cyber risk disclosure in the banking sector, the following section will highlight more related aspects.

1.2 Background to the study

This study aims to compare risk reporting, more specifically cyber risk reporting, between the South African financial markets and those in the Chinese financial markets, focusing specifically on the banking sector.

All listed South African organisations are required by the Johannesburg Securities Exchange (JSE) to comply with the International Financial Reporting Standards (IFRS) as well as the King reports (IODSA, 2010; JSE, 2017). The King III report was the first report that stated that

organisations need to produce an integrated report instead of both a traditional annual financial as well as a sustainability report. King III goes further in saying that listed organisations that fail or choose not to produce integrated reports must give an explanation as to why they are not adhering to this requirement (IODSA, 2010). Integrated reporting states that organisations should disclose what the specific risks they face are, what possible opportunities can arise from these risks are and how they affect the organisation's ability to create value over time (Integrated Reporting Committee of South Africa, 2013).

King IV outlines the requirements for risk governance. Principle 11 states: "The governing body should govern risk in a way that supports the organization in setting and achieving its strategic objectives" (IODSA, 2016). King IV provides a series of recommended risk practices that the governing body of any listed organisation should perform of which more detail will be provided in Chapter 2.

China's financial reporting has to adhere to all the requirements as stipulated by the China Accounting Standards Committee (CASC) (CASC, 2018). China also complies with IFRS reporting requirements (CASC, 2018). The differences in reporting between these two countries will be analysed further in Chapter 2.

1.3 Problem statement

In the business world, business risks have always existed. There have been major corporate scandals that had significant impacts on the financial environment. All of which has led to an increased interest in risk reporting (Oliveira, 2013). It became clear that some banks manage their risks poorly due to weak risk data compiling capabilities and risk reporting practices. This proved to have severe consequences on the banks themselves as well as the stability of the financial system as a whole (Bank for International Settlements (BIS), 2013).

In a study done by Linsley and Shrives (2000) they argue that organisations have become more exposed to volatility and uncertainties (Khlif & Hussainey, 2016:181). Although in recent years there have been many improvements, investors still know too little about an organisation's risks and a risk information gap still exists between organisations and their stakeholders (Wilson, 2014). During the past decade, the determinants of risk-reporting practices have attracted major interest in accounting and finance literature. It has also been found that organisations are reluctant to comply with risk disclosure requirements (Al-Hadi, Hasan & Habib, 2016). In general, larger organisations are more complex and have a wider range of

operations. This implies that they are subject to higher risk levels which translate into higher information irregularities amongst investors (Al-Hadi et al., 2016). Under a mandatory regime, an organisation is required to align itself with mandatory requirements in terms of risk reporting. This means that different organisations that operate under the same mandatory risk-reporting requirement will most likely adopt the same disclosure policy. If multiple organisations adopt the same disclosure policy, there will be almost no variation in disclosure amongst them. The result is that corporate characteristics will not have a major effect on risk reporting under a mandatory regime. When comparing this to a voluntary regime, an organisation will be more inclined to communicate information concerning risk disclosure, especially in scenarios containing high political visibility and high financial risk. Thus, it is expected that the rules of disclosure will strengthen the connection between corporate characteristics and risk reporting (Khlif, Ahmed & Souissi, 2017).

Media platforms report daily on the rampant increase in cybercrime. This has sparked fear in the public eye that cyberattacks would affect national resources and destabilise infrastructure (Berry, 2018). One of the main contributing factors to this naivety is that the Protection of Personal Information Act (POPIA) is not fully in effect. Sophos, an organisation which is a global leader in network security, conducted a study and found that only 34% of South African organisations comply with the POPI Act (Sophos, 2019).

The impact of this is that breaches or service denial attacks on South African organisations are often not reported or made public. This type of publication would attract negative media and public scrutiny, which will have serious consequences on an organisation's reputation. As a result, very few cyberattacks on South African organisations are publicised (Berry, 2018). Between January and August 2018, South African Banking Risk Information Centre (SABRIC) reported that an estimated R250 million was lost due to cyber and digital banking crimes. This is only the reported statistics. Most cybercrimes go unreported (SABRIC, 2019).

As discussed in the problem statement, it seems that risk disclosures in general, but cyber risks specifically, are not reported uniformly between organisations which has led to the objective of this study.

1.4 Objective of the research

1.4.1 Main objective

The main objective of this study is to evaluate the level of disclosure and to compare the practices of cyber risk disclosure in the banking sector between South Africa and China.

1.4.2. Secondary objectives in the literature

- Investigate the attribute of quality reporting.
- Investigate the reporting requirements in South Africa.
- Investigate the reporting requirements in China.
- Indicate the importance to disclose risk information.
- Indicate the importance to disclose risk information in the banking sector.
- Indicate the importance to disclose cyber-risk information in the banking sector.

1.4.3. Secondary objectives in the empirical study is

- to identify the research method,
- to identify the population and the sample,
- to collect data,
- to develop a measuring instrument based on the literature study, and
- analyse the data, and to make recommendations.

The empirical objective is to analyse how the banks have reported on cyber risks in their annual reports. The study will compare the cyber risk elements found in the integrated reports of the South African banks with the reporting practices of the banks in China.

1.5 Research methodology

The research methodology will consist of a literature and empirical study.

1.5.1 Literature study

Research and supporting literature obtained from journals, Google Scholar and EBSCO-host will be used to develop a disclosure index.

1.5.2 Empirical study

1.5.2.1 Research design

The research method utilised will be a content analysis. The research design followed in this study is the mixed method research design. A disclosure index will be developed from the literature studied. This will be used to analyse the results.

1.5.2.2 Population

The population will be all the listed financial service providers (banks) in South Africa and China.

1.5.2.3 Sample

The sampling method used for this study is purposeful sampling, which is where a particular setting is selected specifically for the information that it can provide (Bryman & Bell, 2014). For this study, the banks were selected based on their asset value. China was chosen as it is an emerging economy and along with South Africa, it is part of the BRICS countries (Asongu, Akpan & Isihak, 2018:2).

For the South African market, the four biggest banks were selected based on their asset value. These four banks (FirstRand Bank, Standard Bank, Absa Bank, Nedbank) had a combined asset value of 5 940.6 billion rand in 2018 (454.1 billion dollars) (Businesstech, 2018). In 2017 FirstRand had the biggest headline earnings of 22.4 billion rand and Standard bank has the biggest footprint of all the South African banks (Businesstech, 2017). The purposeful sampling of these banks will represent the majority of the South African banking sector and will remove the possibility of the much smaller banks skewing the findings (Bryman & Bell, 2014).

For the Chinese financial markets, the following four banks in China were selected based on their asset value – the Industrial and Commercial Bank of China, China Construction Bank, Bank of China, and the Agricultural Bank of China. These are the four biggest banks in China, having a combined asset value of 13 637.2 billion dollars (Businesstech, 2018), and according to the British Magazine "The Banker", these banks are also the four biggest banks in the world (Businesstech, 2018; chinaplus.cri.cn, 2018).

The four banks from the South African market together with the four banks from the Chinese market give a total sample size of eight units.

1.5.2.4 Data collection

All the banks chosen for this study have to submit annual financial reports as stipulated by the JSE and CASC (CASC, 2018; JSE, 2017). These annual reports are available for download online.

The data needed for this study will be obtained from the latest annual financial reports and integrated reports from the banks referred to in the above section.

1.5.2.5 Analysis of data

This study will focus on the qualitative and quantitative data included in the annual reports disclosed by the banks on an annual basis and apply a principle component analysis. Descriptive statistical analysis for mean, standard deviation and frequencies will be used to analyse the data compiled from the disclosure index.

1.6 Limitations of the study

This study is descriptive in nature as it will only use the four largest banks in both South Africa and China, with the focus on cyber-risk reporting. The research sample is composed of eight banks, four within South Africa and four within China. The primary data gathering method used was a document analysis/review of the financial reports of the above-mentioned banks. The study uses purposive sampling. An assumption of this study is that the selected banks chosen will represent each country and the assumption is that they successfully represent and reflect the banking industry within each country.

1.7 Proposed chapter layout

Chapter One

The basic background information for the research is presented in chapter one. This chapter is divided into the following sub-sections: introduction, background to the study, problem statement, objectives to the research, research methodology, limitations of the study and proposed chapter layout.

Chapter Two

Chapter two specifically deals with the literature review outlining the related literature used for this study. This includes risk reporting, cyber-risk reporting and reporting by country. This chapter will lay the foundation for the comparative index.

Chapter Three

Chapter three addresses the empirical objectives. This chapter deals with data presentation and analysis of the findings. These will be presented in a graphical and tabular format generated from the findings that were obtained from the document review of the financial reports of the selected banks.

Chapter Four

In chapter four, the findings obtained in chapter three will be discussed alongside recommendations, limitations of the study, suggestions for further research and the conclusion.

1.8 Conclusion

Both South African and China's banks are subjected to different reporting requirements. Over the last few years risk-reporting practices have attracted major interest, specifically cyber-risk reporting. As organisations do not report risks uniformly, the core and value of the matter lies in the reporting practices. In the chapters that follow, this will be explored in more detail, with the focus on cyber risk.

Chapter 2

Literature review

2.1 Introduction

This chapter will focus on the practices of risk disclosure in South Africa and China. This includes the requirements for listed organisations within both countries and the importance of the risk information that is disclosed. The focus will be on the financial sector and specifically cyber risk reporting within the banking sector and why this is important. Further to this, the next section will detail the qualitative attributes of quality reporting and effective financial management.

2.2 The attributes of quality reporting

Most reporting models are limited and do not show all the relevant relationships between elements. As found in previous literature, the accuracy and quality of a financial report is considered an effective tool for conducting feasibility and financial analysis as well as assisting with interpretation of the information disclosed in the annual report (Khlif et al., 2017).

The following are all qualitative characteristics of financial reports (Bragg, 2018):

- Understandability. The information must be easily understood by the users of the financial report. Information must be clearly presented, with supporting references where necessary.
- Relevance. The information must be relevant as it will affect the economic decisions of the user.
- Reliability. The information must be true and unbiased.
- Comparability. The information must be homogenous to preliminary information presented for all accounting periods. This will allow users to identify trends in the performance and financial position of the organisation.

Given the critical role that financial statements play, it is imperative that efforts are made to examine ways to improve their quality, and to understand their purpose and limitations in providing a comprehensive view of an entity's financial position (Choudhury, 2014).

Risk reporting tends to be more non-financial than financial, historic rather than future orientated, good news rather than bad, and qualitative rather than quantitative. When the

relationship between financial and non-financial information becomes better understood, better decisions can be made and as a result, systems and business processes will show an increase in efficiencies and effectiveness (Krzus, 2011).

The current reporting shortcomings have emphasised the need for a more integrated and holistic form of reporting that will not only focus on the economic, environmental and social impacts of an organisation's every day activities, but which will integrate both the financial and non-financial information in a meaningful and integrated manner (Carels, 2014:3; Global Reporting Initiative (GRI), 2018).

The relevant stakeholders in an organisation have a great interest in that organisation's financial reports (Crowther, 2018:7). The reliability and relevance of those reports, as well as the ability to provide sufficient insight, is of great value to them since it helps to enable these stakeholders to make informed decisions that will help the organisation to continue as is, or improve in the future (Carels, 2014:3).

Elshandidy and Neri (2015) postulates that organisations in general do not tend to provide quantitative and forward-looking attributes related to risk disclosure, but qualitative and historical information. Variations in risk disclosure are partially aligned with country related regulations which plays an important role in an organisations incentive. The impacts of risk factors vary by country. In the United States and Canada, an organisation's risk disclosure is positively associated with their risk levels, whereas German organisations are negatively associated with their risk levels and United Kingdom organisations are not significantly related at all (Elshandidy et al., 2018).

Abdullah, Percy and Stewart (2015) found various patterns on how corporate governance affects risk disclosure practices between Islamic and conventional financial organisations. The study further finds that there are various differences in risk disclosure between the Gulf Cooperation Council (GCC) countries, regardless of sociocultural and regulatory similarities.

It can be conclude that the key attributes for effective financial management includes accessibility and completeness, use of information to improve and develop management standards, and assurance that the information is truthful, appropriate and secure, as and when required (Khlif et al., 2017).

The next section will highlight the importance of the risk information that is disclosed to compile quality reports.

2.3 The importance of disclosing risk information

Risk management through all the various industries can be defined as "the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities" (Ata & Schmandt, 2016:6). Risk management methods and definitions vary widely between the various industries.

The latest global survey, conducted by Corporate Compliance Insights, (CCI), of C-level executives and directors of the macroeconomic, strategic and operational risks that organisations face indicates an increasingly risky year ahead. Overall, 825 C-level executives and directors participated in 2019's global study.

The top ten risks identified by CCI, for 2019 are (Deloach, 2019):

1. IT legacy systems – this occurs when existing operations and IT systems cannot meet performance expectations related to quality, time to market, cost and innovation, as well as competitors.
2. Staff turnover – the inability to retain and attract competent personnel.
3. Regulatory changes – may impact the way products or services will be produced or delivered.
4. Cyber risks – threats to the organisation's IT systems that would disrupt core operations and lead to reputational damage.
5. Resistance to change – the unwillingness to adapt within ever-changing environments.
6. New innovations – new technologies within the industry may overtake the ability to compete and manage the risk appropriately.
7. Privacy and security risks – insufficient resources to contain the increasing number of threats.
8. Data analytics – the ability to harness the power of data and advanced analytics to achieve competitive advantage and manage operations more effectively.
9. Cultural risk – the struggle related to differences in language, customs and norms.
10. Customer retention – the inability to adjust to ever-evolving customer preferences and demographic shifts.

As mentioned in point 4, cyber risk was identified as one of the top ten risks. It is of the utmost importance that these risks are reported. The risk reporting requirements in South Africa are discussed in more detail in the following section.

2.4 Risk reporting requirements in South Africa

The origins of South Africa's current reporting requirements can be traced back to 2010. This dates back to the implementation of the International Integrated Reporting Council (IIRC) which was the result of the collaboration between two organisations that led in the field of accounting and sustainability. These two organisations were the Prince of Wales's Accounting for Sustainability project (A4S) as well as the Global Reporting Initiative (GRI) (Flower, 2015:1). The A4S was established in 2004 by the Prince, with the goal to ensure that "we are not battling to meet 21st century challenges with, at best, 20th century decision making and reporting systems" (A4S, 2019). The GRI is an independent international organisation that has pioneered sustainability reporting since 1997 (GRI, 2019). The two organisations have similar goals. The A4S aims for a fundamental shift towards resilient business models and a sustainable economy and the GRI aims to help businesses and governments across the world to both understand and communicate their impact on climate change, human rights, governance and social well-being (A4S, 2019; GRI, 2019). Flower (2015:2) explains that the rationale for the creation of the IIRC was the following:

> "The world has never faced greater challenges: over-consumption of finite natural resources, climate change, and the need to provide clean water, food and a better standard of living for a growing global population. Decisions taken in tackling these issues need to be based on clear and comprehensive information; but, as the Prince of Wales has said, we are at present 'battling to meet 21st century challenges with, at best, 20th century decision making and reporting systems'. The IIRC's remit is to create a globally accepted framework for accounting for sustainability. . . The intention is to help with the development of more comprehensive and comprehensible information about an organization's total performance, prospective as well as retrospective, to meet the needs of the emerging, more sustainable, global economic model."

After the IIRC was formally incorporated in August 2010, the council was tasked with the development and design of a framework that would assist in the compiling of integrated reports produced by organisations (Humphrey, O'Dwyer & Unerman, 2017:31). Flower (2015) clarifies that the IIRC council, at this time, was a partnership of different international auditing

and accounting organisations, stock exchange regulators and senior management of international organisations. These partners developed the final framework in 2013, improving on the initial framework which was released in July 2012 (IIRC, 2012; IIRC, 2015).

The IIRC (2012:7) stated that: "This framework is principle-based. The intent of the principle-based approach is to strike an appropriate balance between flexibility and prescription that recognises the wide variation in individual circumstances of different organisations while enabling a sufficient degree of comparability across organisations to meet relevant information needs".

In 2002 the King II Code on Corporate Governance was released along with its incorporation into the JSE Listing rules and this made South Africa the first country in the world that required organisations to report on both nature and the extent of "social, transformation, ethical, safety, health and environmental management policies" (Setia, Abhayawansa, Joshi & Huynh, 2015). All of this has led to a culture of sustainability (Setia et al., 2015).

In 2009 when the King III Code on Corporate Governance was released, it introduced the requirement for organisations to present integrated reports (IODSA, 2010:48; Setia et al., 2015). The new corporate governance report was incorporated into the JSE listing rules, and if organisations were not able to provide integrated reports they had to say why they were non-compliant (JSE, 2017). The 2009 King III Code stipulates that integrated reporting should enable financial results to be linked to non-financial results, "how the organisation has both positively and negatively impacted on the economic life of the community in which it operated during the year under review" (IODSA, 2010:61; Setia et al., 2015). The Integrated report should also contain information on "how the organisation intends to enhance those positive aspects and eradicate or ameliorate the negative aspects in the year ahead" (Setia et al., 2015). King Code III places great emphasis on organisations reporting the impact that they have on the community (Rossi & Orelli, 2019:14). It further implies that the audience of an integrated report is much wider than those of financial capital providers. As a result, rather than having a value to investors perspective as indicated by the IIRC, this has more of a value to society perspective which stays true to the tradition of sustainability reporting (Setia et al., 2015). All of this shows "the influence of the historical significance of social issues and a long tradition of strong sustainability reporting in the conceptualization of integrated reporting in South Africa" (Setia et al., 2015).

King IV was implemented in 2016. It provides a series of recommended risk practices that the governing body of any listed organisation should perform. KPMG summarised these practices as (KPMG, 2016):

- Set the approach for risk governance, including opportunities and risks when developing strategy and the potential positive and negative effects of the same risk on the achievement of objectives.
- Treat risk as integral part of decision making and adherence to duties, approve risk policy, evaluate and agree the risks it is prepared to take (i.e. risk appetite and risk tolerance levels).
- Delegate to management risk management implementation.
- Oversee the risk management (including assessment of risks and opportunities in relation to the triple context and use of 6 capitals, achievement of objectives, dependency on resources as well as the risk responses, business continuity and culture of the organisation).
- Consider receiving periodic, independent assurance on the effectiveness of risk management.
- Disclose nature and extent of risks and opportunities; overview of the risk management system; areas of focus; key risks, unexpected risks, risks taken outside tolerance levels; and actions to monitor and address risk management.

Another listing requirement is that organisations have to comply with International Financial Reporting Standards (IFRS)(JSE, 2017). As per principal 7 of IFRS, organisations are required to list:

- The significance of financial instruments for the entity's financial position and performance (IFRS, 2018) .
- The nature and extent of risks arising from financial instruments to which the entity is exposed during the period and at the end of the reporting period, and how the entity manages those risks. The qualitative disclosures describe management's objectives, policies and processes for managing those risks (IFRS, 2018).

All listed organisations in South Africa must comply with King IV and IFRS as stipulated in the JSE listing requirements. Refer to appendix A for the complete list.

In the following section the risk reporting requirements in China are discussed, as they differ significantly from that of South Africa, discussed in section 2.4.

2.5 Risk reporting requirements in China

The Chinese securities market really only started in 1990 with stock exchanges set up in Shanghai and Shenzhen. Only 10 organisations were listed. In 10 years, this number grew to 923 organisations and 3584 organisations in 2018 (TGE, 2019).

China's financial reporting had to adhere to all the requirements as stipulated by China Accounting Standards Committee (CASC) (CASC, 2018) until China adopted accounting standards specified by the International Accounting Standards Board (IASB). The Chinese Accounting Standards (CAS) were replaced by the International Financial Reporting Standards (IFRS). This brings China more in line with the rest of the world. The new procedures became law on 1 January 2007.

China complies with various IFRS standards, specifically IFRS 7, as stated in section 2.4 above, which is a requirement for risk reporting. IFRS 7 requires entities to provide disclosure in their financial statements that enables users to evaluate the significance of financial instruments as well as the risks arising from these financial instruments (IFRS, 2018). This is similar to the South African reporting requirements as stipulated by the JSE.

The China Banking Regulatory Commission (CBRC) adopted regulations which came into effect 1 January 2013. According to these regulations, all China's commercial banks are required to disclose information related to exposure and evaluation of credit risk, operational risk, market risk and any other relevant risks, as well as risk management (Wang, Chen & Zhao, 2018:2). From the above it is clear that organisations in China's banking sector have to comply with both IFRS and CBRC regulations.

The following section will point out why these reporting regulations have been implemented and specifically why risk disclosure is of such vital importance.

2.6 The importance of disclosing risk information in the banking sector

A key finding, after the global financial crisis that started in 2007, was that information technology and data architecture in the banking sector was severely lacking and unable to support the broader management with financial risks (BIS, 2013:8). The majority of banks lacked the ability to combine their risk exposures and detect risk concentrations quickly and accurately at a bank group level, across business lines and between legal entities (Thun, 2015).

Some banks managed their risks poorly due to weak risk data compiling capabilities and risk reporting practices. This proved to have severe consequences to the banks themselves as well as the stability of the financial system as a whole (BIS, 2013). As mentioned before, traditionally the management of risk is done on a standalone basis. This means that they are also unaware of the potential impact these risks from other departments could have on them and if these risks could have been avoided or capitalised on (Ata & Schmandt, 2016:11).

In the following paragraphs a few past events of risk management failures, within the banking sector, will be highlighted to provide a background of what went wrong in these institutions.

Wells Fargo

Wells Fargo is a prime example of poor risk reporting. Leading to consequences of $185 million in penalties and 5 300 employees being fired (Craddock & West, 2018:18; Tayan, 2019:2). The incident better known as the "Wells Fargo cross selling scandal" originated in 2013 when employees unlawfully opened up millions of accounts which generated overdraft charges and other fees (Sovern, 2017:418).

On 16 December 2009, the Securities and Exchange Commission (SEC) adopted amendments to its disclosure rules and forms to enhance the information provided to shareholders so they are better able to evaluate the leadership of public organisations. The amendments are intended to improve disclosures regarding risk (SEC, 2012). In 2010, the SEC's Proxy Disclosure Enhancements (rule 33-9089) made boards accountable for disclosing a variety of threat management requirements by establishing an Enterprise Risk Management (ERM) mandate for corporations. Notable obligations include (SEC, 2012):

- The disclosure of risk management effectiveness and systems used to manage risk.
- The board's role in risk oversight and in-depth knowledge of the organisation's material risks.
- Analysis of its incentive scheme for employees. What this means is organisations cannot put employees in a risk versus reward trade-off position.

Wells Fargo did not comply with SEC's amendments and as a result of the unrealistic sales the targets were not reported, and the risks were overlooked.

The Leman Brothers

The Leman Brothers is another example of why risk reporting is important. The Leman Brothers was, prior to the 2008 financial crisis, the fourth largest investment bank in the United States, but due to poor risk management decisions filed for bankruptcy in September 2008 (Koshy, 2018:13).

The Lehman Brothers overlooked their risk management. This was the main reason why they failed as they refused to look at the truth behind the unrealistically large profits they were making from mortgage-backed securities (McDonald, 2013).

There were clear cut signs prior to the financial crisis that their risk exposure was too high.

Looking at the 2007 year-end financial statements, their current ratios were low, indicating high liquidity risk. Their leverage ratio was high indicating that they had too little equity capital should they incur losses on the balance sheet (Harris, 2013:91). Madelyn Antoncic, chief risk officer at the time, told the CEO that the organisation was "too risky" (McDonald, 2013). They simply chose to ignore all the signs.

Swiss bank UBS

The Swiss bank UBS lost $2.3 billion due to a rogue trader in its London-based investment banking arm (Thomasson, 2011). The 67-year-old CEO at the time, Mr. Oswald Grubel, made a statement in a memo after he resigned:

> "That it was possible for one of our traders in London to inflict a multibillion loss on our bank through unauthorised trading shocked me." (Thomasson, 2011)

When an investigation was launched to see how this happened it was found that UBS failed to act on the warning signs and as a result could not prevent the loss (Amery, 2012; Lee, 2011). The investigation showed that there was a shortage in risk measures as the risk management system of the trader was inadequate and even though the central risk systems of UBS were throwing out warnings of unauthorised trading, these indicators were ignored (Amery, 2012; Lee, 2011).

Thomas O. Gorman, a partner at Dorsey & Whitney L.L.P. in Washington, after receiving news of the UBS scandal said: "One has to wonder why the tell-tale signs for one reason or another were missed" (Greenwald, 2011).

A risk management consultant, James Lam, president of James Lam & Associates Inc, said a governing structure is needed to prevent, or at least minimise, the risk of rogue trading (Greenwald, 2011). He also described such an individual as a risk officer with the authority: "to challenge key business lines ... all the way down to individual business units and back-office operations, to make sure the right people are in place to provide the checks and balances" is what is required (Greenwald, 2011).

The rogue trader from Swiss bank UBS manipulated the system by using forward settling and exchange traded funds (ETF) cash positions to hide the trades and make them near impossible to detect. European ETF transactions do not issue confirmations until the transaction gets settled. By exploiting this characteristic it allowed for the party to receive payment before the transaction settled (Amery, 2012). The rogue trader made use of a false hedge trade to hide the fact that he was in breach of his risk limits. This did generate a loss which was on its own manageable, however, the sum of all the losses created net loss for UBS which was picked up in that following financial quarter report (Lee, 2011).

It came to light that the checks and balances were overlooked. The manager of the rogue trader overlooked the illegal trading, he was also aware the trader was over his risk limits. Further investigation showed the manager was also aware of a profit pool his trading team as a whole used to hide their losses (Wilson, 2014). But the size of this loss made by the rogue trader was too large to hide, the rogue trader was jailed for seven years and the manager was fired as well as banned by the Financial Conduct Authority (FCA) from working in the financial sector ever again. Tracey McDermott, the Director of the FCA stated:

> "He should have been acting as a role model to others. Instead he failed to report the Umbrella and allowed the desk's profit and loss to be misstated over an extended period" (Wilson, 2014).

From the 3 examples discussed it becomes clear how important proper risk management procedures are in an organisation. Wells Fargo and UBS fell short in this aspect as they did not have appropriate risk management procedures in place. Furthermore, risk management is a crucial tool and should be used. There is no value to a proper sophisticated risk management process if it is not used. The Leman Brothers and UBS are prime examples of this as they both had the risk management tools in place but management chose to ignore it. Had the risks been

reported to the relevant people, the huge reputational damage and financial losses could have been minimised or even avoided.

It is evident following the examples provided as to why risk disclosure within the banking sector is of such vital importance. Section 2.7 will focus specifically on cyber risk and why it has become one of the top-rated risks in the banking sector.

2.7 The disclosure of cyber risk information in the banking sector

As the world's people, finances and knowledge become indistinguishably linked, an occurrence that is referred to as globalization and interconnectivity becomes more visible. The previous global financial crisis is evident of this (IIRC, 2018).

As competition becomes more challenging and environmental concerns continue to grow, organisations need to find ways to differentiate themselves from the masses. Businesses need to start looking at ways to change the norm when it comes to reporting, facilitating and communicating mega-trends by eliminating the complexity and shortages of the current reporting requirements (IIRC, 2018). Technology is advancing at such a rapid pace, that to be able to remain both authentic and relevant can prove to be quite a challenge. Transparency, compliance and ethics are continuously evolving, while corporate governance still remains a key element in any business (Vieru, 2017). Organisations are not only relying more on digital technology to conduct their business operations but also as a means to engage with their customers, their business partners, and other constituencies (Securities & Commission, 2018:2). This technological advancement and digital connection in the world have presented some risks. Cyber security is an ever present ongoing risk to all markets and industries (Securities & Commission, 2018). As the banking sector is highly advanced in technology and relies on digital connections, the sector is vulnerable in terms of cyber risk (Bouveret, 2018)

Concern has grown about cyber security over the last few years. Businesses are especially concerned as this risk could lead to substantial costs , as well as various other implications such as exposure of sensitive personal information, business disruptions, remediating costs, increased cyber security protection cost, litigation and legal risk, reputational damage, or even theft of trade secrets (Li, No & Wang, 2018:40; Securities & Commission, 2018:4). Bouveret (2018) tried to determine which countries were more exposed to cyber risk and he found that the financial sector across all countries are all highly exposed. In 2018 cyber security played an important role in the Securities and Exchange Commission's (SEC) regulatory agenda, the

commission published an interpretive guideline that urges companies to be: “more transparent in disclosing cyber security risks in their public filings; to disclose material data security incidents in a timely fashion; and to implement safeguards such as trading bans to prevent insiders from selling securities after a breach is detected but before it is publicly disclosed” (Newman & Belknap, 2019). The SEC advises organisations to consider several factors when preparing cyber risk disclosure (Newman & Belknap, 2019):

- all prior cyber security incidents including their severity and frequency;
- the probability of an incident occurring and what the impact is of such an incident;
- the limitations of an organisation’s ability to mitigate cyber risk;
- any industry specific or third-party risks;
- the potential of reputational harm; and
- the legal risks and costs of enforcement actions by other regulatory bodies.

The goal of the pre-incident public disclosures is to provide a rounded assessment based on the complete materiality of cyber risk to an organisation and how it affects their operations.

Cyber risk can be defined as “operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems” (Bouveret, 2018). When looking at risk characteristics and categories that are insured, cyber risk shares similar characteristics with property and liability risk, and also catastrophic and operational risk (Eling & Wirfs, 2016). Cyber risks have been found to have severe impacts both directly on an organisation and indirectly as it affects third parties, it is also known that losses that have occurred from cyber risk have been found to be significant (Bouveret, 2018). In a study done by Cavusoglu, it was found that a cyber security breach could negatively affect an organisation’s share price by up to two and a half percent (Eling & Schnell, 2016:477). There are studies that show that a breach in confidential data has an even more severe impact on the organisations share price (Eling & Schnell, 2016:478). However, not all cyber risks are related to cyber-attacks or “hacks” which are malicious, some occur due to business disruptions such as software updates. These are referred to as cyber incidents (Bouveret, 2018). Cyber-attacks can affect the organisation through three main aspects of information security which are: confidentiality, integrity and availability. Confidentiality issues occur when private information within an organisation is disclosed to third parties, this is usually as a result of data breaches. Integrity issues imply abuse of systems, this is related to

fraud and theft. Availability issues are related to business disruptions. There may be various causes responsible such as, infrastructure failure and software related issues (Bouveret, 2018; Kaffenberger & Kopp, 2019).

Business disruptions hinders organisations from operating, resulting in lost revenue, fraud and theft leads to financial losses, while the effects of data breaches materialise over a longer period. All of these causes reputational damage and possible litigation costs (Bouveret, 2018:4). The loss of confidence following a cyber-attack could be significant for the financial sector, given the reliance of financial institutions on the trust of their customers. Regarding the financial system, business disruptions are more likely to have a direct short-term effect, than fraud and theft or data breaches (Bouveret, 2018:4; Warren, Kaivanto & Prince , 2018:28).

2.8 Conclusion

From the above it is evident that cyber risk is one of the most prominent threats in the banking sector. It is mandatory for both countries to report on cyber risk, however, the quality, value and significance of this reporting between the two countries, is still unclear, as their reporting requirements differ. China does not adhere to the same reporting requirements as South Africa and as such, the lack of critical information may leave the organisation vulnerable. To determine the differences in quality and value of the reporting methods used by both countries, a disclosure index will be constructed to assist in revealing the differences in quality and value.

The following chapter will discuss the research methodology as well as identify the criteria for comparison in the disclosure index. It will also discuss the content analysis procedure which will be used to analyse and evaluate the findings obtained from the disclosure index.

Chapter 3

Research methodology

3.1 Introduction

This chapter discusses the research methodology used in this study. It points out the relevant information that was identified in the literature from the previous chapters and uses this as a guide to compile the disclosure index, which will be focused around cyber risk reporting. The findings of this table will be further supported with a quantitative analysis.

3.2 The research approach

This study will comprise of a mixed method approach, which is a combination of both the quantitative and qualitative research methods. The mixed method approach can be defined as:

> ‘‘research in which the investigator collects and analyses data, integrates the findings and draws inferences using both qualitative and quantitative approaches” (Östlund, Kidd, Wengström & Rowa-Dewar , 2011; Tashakkori & Creswell, 2007:7).

This approach tries to draw upon the strengths and perspectives of both qualitative and quantitative methods and how things appear in its natural state along with how it is influenced by external forces such as human intervention (Johnson & Onwuegbuzie, 2004; Östlund et al., 2011). The combining of qualitative and quantitative research methods can assist in highlighting the differences and similarities between the particular aspects of a data set (Bernardi, Keim & Von der Lippe , 2007; Östlund et al., 2011).

The annual reports released by the banks contain both financial and non-financial information which will be further analysed with statistical methods. The next section shows how the data was collected to accommodate the research approach.

3.3 Data collection

The data collection method used in this study is document analysis. This form of analysis is a systematic procedure used to review and evaluate documents that contains text and images that have been recorded without any intervention from the researcher or external sources. Document

analysis requires that data be examined and interpreted to draw meaning and gain understanding in order to further develop empirical knowledge (Bowen, 2009:27).

The analytical procedure, when applying document review, includes identification, selection, appraising and synthesizing the data contained within the document (Dietz, Börner, Förster & Von Braun, 2018:8). This data will further be organised into categories by means of content analysis which will be discussed in section 3.4.

3.4 Data analysis

Content analysis will be applied when compiling the data from the document review. Riff (2019) defines content analysis as:

> "Quantitative content analysis is the systematic and replicable examination of symbols of communication, which have been assigned numeric values according to valid measurement rules and the analysis of relationships involving those values using statistical methods, to describe the communication, draw inferences about its meaning, or infer from the communication to its context, both of production and consumption".

Bengtsson (2016), states that when conducting content analysis, five key factors need to be considered; "the aim, the sample and unit of analysis, the choice of data collection method, the choice of analysis method and the practical implications". This outline was used as the guideline for this study.

3.4.1 The aim

The aim is meant to determine the structure of the study design and to set the boundaries (Bengtsson, 2016:10). The aim for this study is to compare the practices of cyber risk disclosure between the two counties, South Africa and China, solely focusing on the banking sector.

3.4.2 The sample and units of analysis

The sample size was based on "The big four" South African banks. Similarly, four Chinese banks were chosen. These banks were chosen based on their asset value and will be seen as representatives for all the other banks in their respective countries.

3.4.3 The choice of data collection method

All the banks chosen for the study are required to produce annual reporting as stipulated by their country's listing requirements (CASC, 2018; JSE, 2017). This documentation is publicly

available and can be accessed on the banks respective web pages. The study focusses on cyber risk related information obtained from these reports.

3.4.4 The choice of analysis method

Data analysis aims to provide meaning from the data collected as well as to draw realistic conclusions from it (Bengtsson, 2016). Content analysis is unique in that it has both a quantitative and a qualitative approach (Bengtsson, 2016). The extent of cyber risk reporting will be illustrated by means of a disclosure index. This index will be built around key concepts such as general reporting information, governance of risk and all information pertaining to cyber risk. The disclosure index will further be used to point out differences between both forms of reporting and complimented by means of a basic statistical analysis.

3.4.5 Practical implications

The data is drawn from only the annual reports. To determine which bank has better cyber risk practices it would be optimal to compare reports that comply with a single governing body. As these countries comply with their own governing bodies, focusing solely on the annual reports might not be optimal. A broader scope of reports such as annual financial statements, risk and capital management reports, environmental social and governance reports, report to society and the general annual report, may result in a more holistic finding.

In the next section the different sub-headings as identified in the literature are grouped into categories and become part of the disclosure index which will then be discussed.

3.5 Items identified to disclose

The sections below will discuss the different sub-headings of the disclosure index. This section will show the generic differences in reporting requirements between the banks chosen for this study, then move on to the governance practices used by the chosen banks, more specifically the governing of cyber risks and the importance thereof in the banking sector. Sections 3.5.3 that follows will look at cyber risk rankings, reporting of cyber risk incidents, their causes, as well as their respective impacts, and lastly risk mitigation procedures in general.

3.5.1 General information

Both countries chosen for the study must comply with different reporting requirements. South Africa is subject to the JSE listing requirements, which includes IFRS and King IV (JSE, 2017). To produce an integrated report is one of the requirements as per King IV. King IV also requires organisations to provide reasons for not submitting integrated reports (IODSA, 2016).

China is subject to the CASC listing requirements, which includes IFRS and CBRC (CASC, 2018). Cyber risk reporting is a legal requirement through specific laws in South Africa and China (Ning & Wu, 2019; SEC, 2012). A requirement for both IFRS and King IV is the disclosure of all risks (IFRS, 2018; IODSA, 2016). Based on this information the disclosure index will address the following:

- Does the bank produce an integrated report?
- Which rules and regulations the bank adhere to?
- Are the rules of reporting cyber risks mandatory or not?

3.5.2 Governance of risks

Government Gazette, No. 35950, sub-regulation 17 states the following: "achieves the objectives relating to sound corporate governance and effective risk management, and complies with the relevant minimum requirements specified in regulation 39". This covers the maintenance of risk management processes, management of material exposures to risk, and reporting requirements for material information technology and cyber incidents (SARB, 2012; SARB, 2019).

As per Principal 11 of King IV: "The governing body should govern risk in a way that supports the organisation in setting and achieving its strategic objectives" (IODSA, 2016:61). This entails that the governing body should assign the responsibility of implementation and risk management to a responsible individual. Risk should be managed as an integral part of the company's day to day activities (IODSA, 2016:61).

The cyber security law in China came into force on 1 June 2017. Under the cyber security law network, operators are required to appoint a designated person in charge of cyber security. All cyber security incidents must be monitored and recorded (Ning & Wa, 2019).

Information technology security policy is a documented set of rules that addresses security vulnerabilities. It further provides guidelines on prevention and mitigation procedures. It also provides guidelines for employees to follow. Every organisation, regardless of size, should have a documented information technology security policy. This policy sets out strict procedures should a security breach result in a lawsuit (Pourkhomami, 2018). In most countries, such as South Africa and China, organisations must comply with various regulations as stipulated by relevant organisations.

There are three core objectives of information technology security policies (Pourkhomami, 2018):

- Confidentiality – protecting information technology assets and networks from unauthorized users.
- Integrity – the amendment of information technology assets should be handled in a specific and authorized manner.
- Availability – ensuring information technology assets and networks are always accessible by authorized users.

By defining cyber risk, organisations gain a common understanding of the subject and fully understand what it entails. From here, an organisation can develop processes to manage and mitigate (Oxford, 2019; Whitfield, 2012).

As mentioned in the previous paragraphs, risk needs to be governed. Therefore, under the sub-heading of "Governance of risk" the following questions will be considered:

- Does the bank have a policy on risks reporting in general?
- Does the bank have a cyber risk policy?
- Does the board of the bank take ownership of risks?
- Do they refer to any strategy related to managing cyber risks?
- Does the bank define cyber risk clearly?
- Does the bank identify cyber risk as a material item?

3.5.3 Ranking of cyber risk

Organisations such as Forbes and the World Economic Forum lists cyber risk as one of the top 10 risks (Demrovsky, 2019; Fleming, 2019). Businesstech ranks cyber security as 9th in the listed risks affecting the South African economy (Businesstech, 2019). Laws in China regulating cyber risk were only implemented in 2017. As such, there is no clear indicator of where cyber risk rates in the Chinese business environment (KPMG, 2017:4). Based on the literature above, it is relative to investigate how the banks rate the importance of cyber risk. The "Ranking of cyber risk" section will look at the following two questions:

- Does the bank rate cyber risk as one of their top ten risks?
- If ranked, how important is cyber risks to the bank?

3.5.4 Reporting of cyber risk incidents

The South African Reserve Bank has issued a new directive 2/2019 in terms of Regulation 39 of the regulations relating to the Banks Act 94 of 1990. The directive sets out the reporting requirements for cyber incidents. The Protection of Personal Information Act (POPIA) was introduce in 2013 and after it comes into full effect, section 22 of POPIA requires that any data breach or suspected breach must be reported to the information regulator and the affected parties. Under the Cyber Crimes Act, the incident must be reported within 72 hours.

In accordance with the Chinese Cyber security Law, organisations will notify the relevant authorities of any cyber incidents within 24 hours. If the publication of such an event will jeopardise China's national security, then such information will be withheld. As with the POPI Act, Chinese Cyber security Law requires organisations to notify affected users in case of disclosure and damage or loss of user information.

Currently, relevant laws and regulations in China do not provide specific requirements about the nature and scope of information to be reported. This is similar to King IV where there are no clear reporting requirements and limited guidance for reporting cyber incidents. We will be considering the following question under "Reporting of cyber risk incidents":

- If there was a cyber risk incident, was this cyber risk incident reported?

3.5.5 Causes of cyber risk incidents

Banks face many types of cyber security threats which fall within these three categories (Tylor, 2018):

1. Financial gain
2. Disruption
3. Espionage

Virtually every cyber threat can be categorised as one of these three types. With current technology there are an abundance of methods to initiate an attack. Below is a list of the ten most common types of cyber threats:

1. Malware. This is software that gains access to a computer as an attachment to a document or photo. The objective of the malware is to take control of the computer or network and to corrupt data (Regan, 2019).

2. Phishing. This is an attack launched through email. The reader is tricked into accessing a link to a supposedly legitimate website in order to obtain personal and confidential information. Alternatively, malware is installed onto the computer through clicking on a hyperlink in the email message (Norton, 2019f).

3. Spear Phishing. The victim is targeted in a way that masks the attacker and impersonates someone known or trusted to the victim. This is done to obtain personal information and to extort money (Norton, 2019g).

4. "Man in the Middle" (MitM) attack. The attacker is in a position between the recipient and sender to intercept electronic messages. The messages are decrypted, possibly altered and then relayed to the recipient. The communication is believed to be directly with one another. This method is used to intercept login or personal information, to spy on someone and to sabotage communications and data (Norton, 2019c).

5. Trojans. It is malicious code or software that can take control of your computer once installed. It is disguised as legitimate software. Users are tricked by some form of baiting into loading Trojans onto their systems. The malware is designed to disrupt, damage or steal data (Norton, 2019d).

6. Ransomware. A hacker gains access to a computer and installs code that encrypts data on the system. He then demands a ransom in exchange for access to the data. These attacks range from low-level incidents to serious attacks which result in an entire organisation's system being locked down (Norton, 2019e).

7. Denial of Service Attack or Distributed Denial of Service Attack (DDoS). This is a targeted attack on a single system. A DDoS attack is an attempt to disrupt data traffic of the targeted server or network. Multiple compromised computers are used as sources of traffic. The objective is to generate enough traffic to the targeted system which will exhaust target resources and cause the server to crash (Cloudflare, 2019; Norton, 2019b).

8. Attacks on Internet of Things (IoT) Devices. Some examples of consumer connected devices are smart tv's, toys, watches and other smart appliances, commercial security systems and systems used to monitor traffic and weather. These devices are vulnerable to cyber threats. Hackers gain access to the device to make it part of a DDoS attack. They gain unauthorized access to data collected by the device. IoT devices are very common across the world. From their numbers and geographic distribution, these devices are a prime target for malicious attacks (Mzekandaba, 2019).

9. Data Breaches. A data breach is where personal information is accessed without authorization. Motives include crime such as theft or blackmail, or to publicly embarrass a person or institution, as well as espionage (Norton, 2019a).

10. Malware on Mobile Apps. Mobile devices are just as vulnerable to malware attacks as computing hardware. Malware is embedded in app downloads, phishing emails and text messages. If a device is compromised, the hacker can gain access to personal information, location data and financial records (Regan, 2019).

3.5.6 The impact of cyber risk incidents

A successful cyber-attack can cause serious damage to an organisation. It impacts on an organisation's bottom line, the organisation's standing and consumer trust. The impact of a cyber-attack can be divided into three categories which will be considered in the disclosure index (Cruickshank, 2019):

- Damage to the reputation
- Financial losses
- Legal actions or implications. What was the impact of these incidents?

3.5.7 Mitigating procedures

A risk mitigation strategy is an action plan that organisations create after they have made a thorough evaluation of possible threats that can affect the organisation. The purpose of such a

strategy is to minimise or ideally prevent adverse impact before any damage or disaster takes place (Cantoria, 2019). The following question will be considered:

- Is a mitigation procedure in place?

The following section looks at how the level of disclosure was determined.

3.6 Level of disclosure

The level of disclosure aims to show how much information each organisation discloses on cyber risk. Previous studies have raised concerns on the unit of analysis that is used to determine the amount of disclosure even though it is common practice to use words or sentences (Amran, Manaf Rosli Bin, Che Haat Mohd Hassan, 2009). Linsley & Shrives (2006) argued that it is difficult to determine which words can be used to estimate risk disclosure, however, early studies done by Hackston & Milne (1996) and later copied by Linsley & Shrives (2006) indicate that using either sentences, words, graphs or columns all yield similar results. For this study a word search for all cyber related phrases was done to determine the level of disclosure.

Following the discussion on the levels of disclosure, details concerning the disclosure index is displayed in the next section.

3.7 Disclosure index

The disclosure index is built around the reporting requirements as indicated by the IIRC, as well as CASC and the Chinese Cyber security Law requirements. This study is systematic and fully replicable. The disclosure index as shown in Table 3.1 is used to measure the disclosure practices of the banks. The numeric values assigned are derived from the observations of the index. Should something be true, or "Yes", a numeric value of 1 would be assigned to that observation. Should something be false, or "No", a numeric value of 0 would be assigned. In cases where no value could be assigned due to the requirements of the criteria not being met, the field was assigned a not applicable (N/A). Table 3.1 is the presentation of the measured criteria from each of the banks' annual reports.

Table 3.1: Cyber risk disclosure index

	FirstRand	Standard Bank	Absa Bank	Nedbank	Industrial & Commercial Bank of China	China Construction Bank	Bank of China	Agricultural Bank of China
General information								
Does the bank produce an integrated report (Yes/No?)	Yes	Yes	Yes	Yes	No	No	No	No
Which rules and regulations does the bank adhere to:								
IFRS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
KING IV	Yes	Yes	Yes	Yes	No	No	No	No
Is cyber risk reporting mandatory?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Governance of risk								
Does the bank have a policy on risks reporting in general?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Does the bank have a cyber risk policy?	Yes	No	Yes	Yes	No	No	No	No
Does the board of the bank take ownership?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Do they refer to any strategy related to manage cyber risks?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Does the bank define cyber risk clearly?	Yes	No	Yes	Yes	No	No	No	No
Does the bank identify cyber risk as a material item?	No	Yes	Yes	Yes	No	No	No	No
Ranking of cyber risk								
Does the bank rate cyber risk as one of their top ten risks?	No	No	Yes	Yes	No	No	No	No
If ranked, how important is cyber risks for the bank?	N/A	N/A	1	2	N/A	N/A	N/A	N/A
Reporting of cyber risk incidents								
If there was a cyber risk incident, was the cyber risk incident reported?	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
CAUSES OF CYBER RISKS INCIDENTS								
Was the cause identified, for example:								
Malware	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Phishing	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Spear Phishing	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Man in the Middle	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Trojans	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Ransomware	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Denial of Service Attack	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Attacks on IoT devices	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Data Breaches	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Malware on mobile apps	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
The impact of cyber risk incidents								
A description of the impact on the bank:								
Damage to the reputation	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Financial losses	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Legal actions or implications. What was the impact of these incidents?	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Mitigating procedures								
Is a mitigation procedure in place?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

In the following sections each of the sub-headings' results will be discussed.

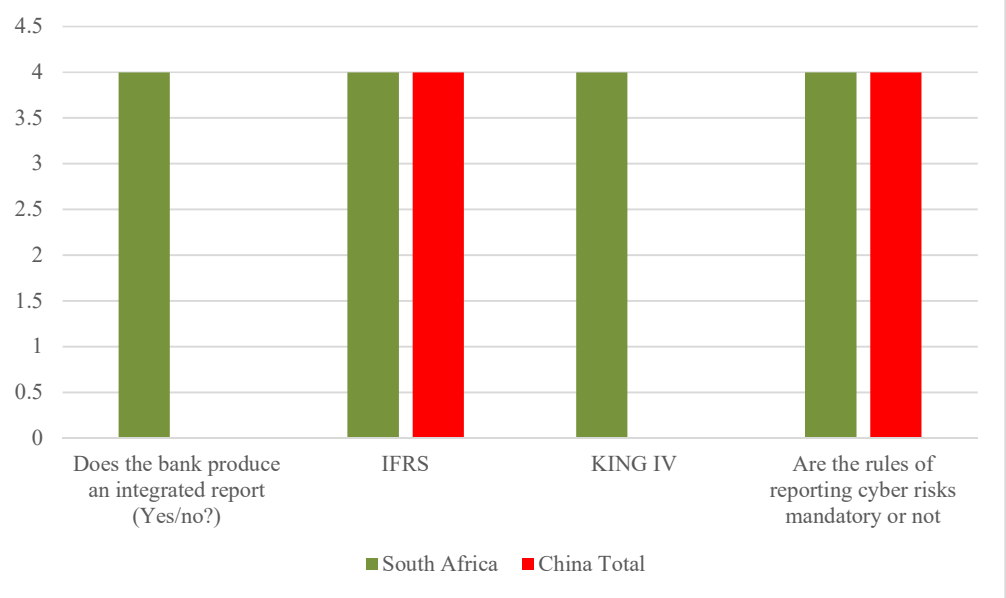
3.7.1 General information analysis

This section looks at the general information collected from the annual reports.

Table 3.2: General information analysis

General information	Compliance Percentages
Does the bank produce an integrated report?	50%
Which rules and regulations does the bank adhere to:	
IFRS	100%
King IV	50%
Is cyber risk reporting mandatory?	100%

When analysing the results about the general information, 50% of the banks in the sample produce integrated reports. All the banks complied with IFRS reporting standards and only 50% complied with King IV regulations. This indicated that half the banks within the total sample must comply with different reporting regulations, although all the banks are required to report on cyber risk incidents. This is illustrated in Graph 3.1



Graph 3.1: General information

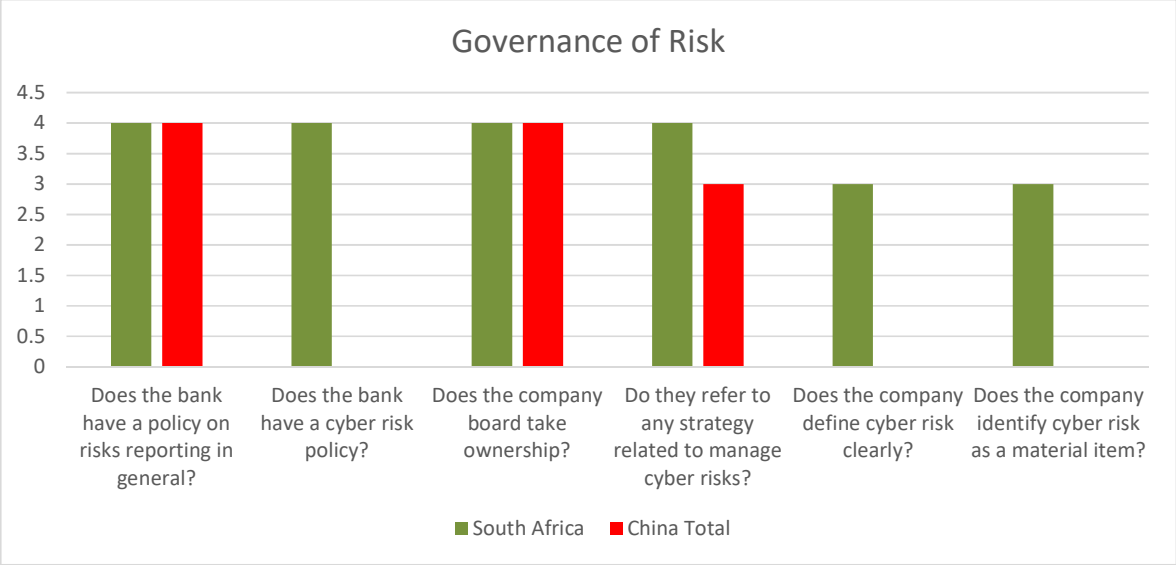
3.7.2 Governance risk analysis

This section looks at the extent to which risks are governed by the bank.

Table 3.3: Governance risk analysis

Governance of risk	**Percentages**
Does the bank have a policy on risk reporting in general?	100%
Does the bank have a cyber risk policy?	38%
Does the board of the bank take ownership of managing risk?	100%
Do they refer to any strategy related to manage cyber risks?	88%
Does the bank define cyber risk clearly?	38%
Does the bank identify cyber risk as a material item?	38%

When analysing the governance of risk, six questions were asked. These questions yielded mixed results. All the banks had a risk reporting policy in place but only 38% had a cyber risk policy. When asked if the bank defined cyber risk clearly, only 38% had a clear indication of what cyber risk relates to and 88% of all the banks had implemented strategies to manage cyber risk. Additionally, 38% of the banks identified cyber risk as a material item, including Standard Bank, however, Standard Bank does not define cyber risk in their reporting. This is conflicting and could indicate that cyber risk incidents reported by them could relate to a wider range of concerns than assumed in general. From the six questions only, Absa and Nedbank both scored 100% compliance. When looking at corporate governance and the sample as a whole, the banks yielded a 67% compliance rate for the specific questions asked. Graph 3.2 summarises the above and illustrates it by country.



Graph 3.2: Governance of Risk

3.7.3 Ranking of cyber risk analysis

This section looks at the cyber risk ranking within the banks.

Table 3.4: Ranking of cyber risk analysis

Ranking of cyber risk	**Percentages**
Does the bank rate cyber risk as one of their top ten risks?	25%

When looking at risk rankings and how banks ranked their risks, only 25% provided a ranking for the risks they faced. The two banks, who provided cyber risk rankings, rated cyber risk amongst their top three risks.

3.7.4 Reporting of cyber risk incidents analysis

This section looks at any cyber risks incidents along with the cause of these incidents and if they were reported.

Table 3.5: Reporting of cyber risk analysis

Reporting of cyber risk incidents	**Percentages**
If there was a Cyber risk incident, was cyber risk incident reported?	0%
CAUSES OF CYBER RISKS INCIDENTS	
Was the cause identified, for example:	
Malware	
Phishing	
Spear Phishing	
Man in the Middle	
Trojans	
Ransomware	
Denial of Service attack	
Attacks on IoT devices	
Data Breaches	
Malware on mobile apps	
What was the impact of these incidents	
A description of the impact on the bank:	
Damage to the reputation	
Financial losses	
Legal actions or implications. What was the impact of these incidents?	

For the 2018 financial year there were no cyber risk incidents confirmed in the annual reports. This might be a limitation of the annual reports and such incidents might be found in additional reports.

3.7.5 Mitigating procedures analysis

This section identifies if the banks have mitigation procedures in place for risks in general.

Table 3.6: Mitigation procedures analysis

Are mitigating procedures in place	**Percentages**
Is a mitigation procedure in place?	100%

All the banks have stated that they do have risk mitigation procedures in place. Very few specifically referred to cyber risk mitigation procedures. The assumption was made that if there was mentioned of risk mitigation procedures, there would be cyber risk mitigation procedures as well.

The next section looks at the levels of disclosure between South Africa and China in terms of cyber risk reporting.

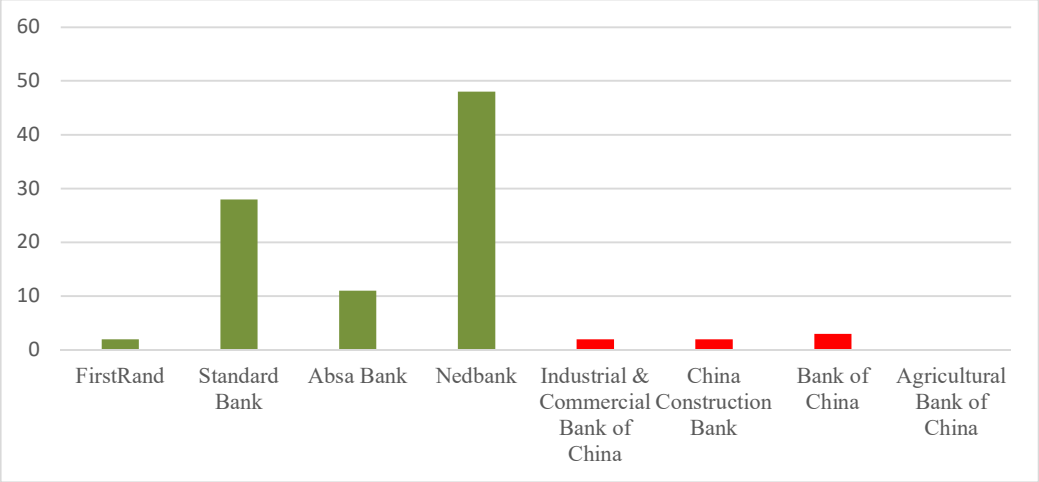
3.8 Level of disclosure analysis

This section indicates the level of disclosure per bank.

Table 3.7: Level of disclosure

Disclosure	**FirstRand**	**Standard Bank**	**Absa Bank**	**Nedbank**	**Industrial & Commercial**	**China Construction Bank**	**Bank of China**	**Agricultural Bank of China**
Cyber term search	2	28	11	48	2	2	3	0

It was found that the South African reports yielded a higher level of disclosure based on a word search analysis that was applied to evaluate how many times all related cyber terms appear in the annual reports. This includes “cyber risk”, “cyberrisk”, “cybercrime”, “cyber security” and “cybersecurity” to name but a few. With regard to the South African banks, Nedbank had a count of 48, Absa had a count of 11, Standard Bank had a count of 28 and FirstRand Bank had a count of only two. The China banks yielded a much lower count with the Industrial and Commercial Bank of China showing a count of two, the Bank of China having a count of three, the Agricultural Bank of China having a count of two and the China Construction Bank not referencing any of the terms at all. Graph 3.3 illustrates the differences on a bank level more clearly.

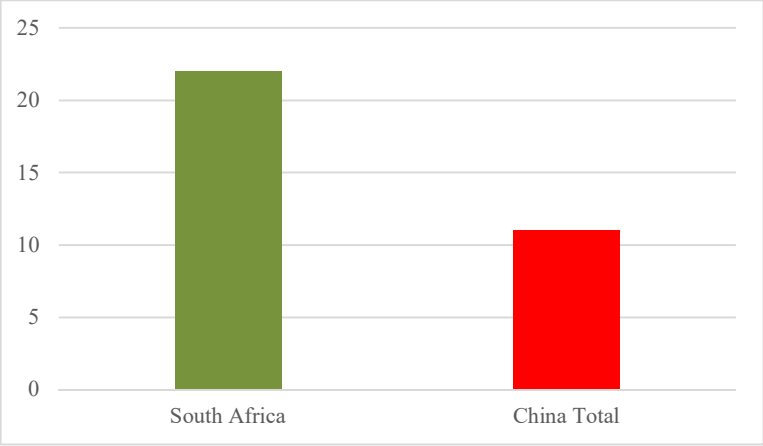


Graph 3.3: Level of disclosure per bank

The next section summarises the differences of the disclosure index between South Africa and China in terms of cyber risk reporting.

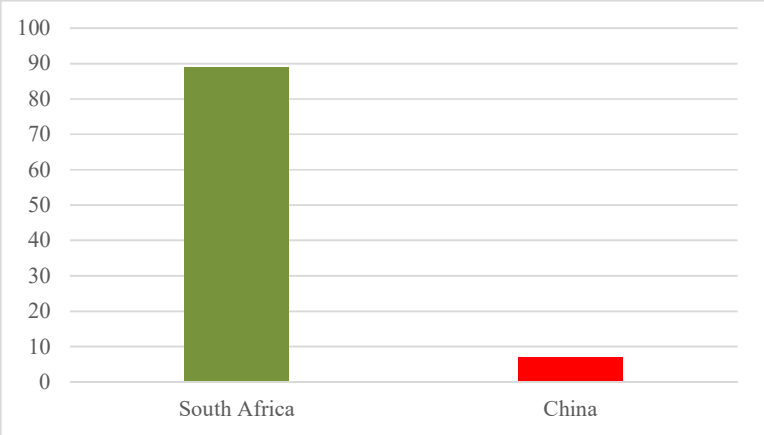
3.9 Conclusion

The disclosure index for the eight banks was based on all of the mentioned categories. The graphs show a significant difference between the observed results of both countries. Graph 3.4 illustrates the total level of compliance for the six risk governance questions per country. The graph indicates a higher level of compliance for South African banks.



Graph 3.4 Governance compliance per country

Graph 3.5 indicates the level of disclosure per country. Nedbank yielded the highest level of disclosure overall and along with Standard Bank and Absa, had a disclosure level of at least 3 times that of all the other banks.



Graph 3.5 Level of disclosure per country

The findings and conclusions will be discussed further in Chapter 4.

Chapter 4
Conclusion

4.1 Introduction
This chapter will present a summary of the findings from the empirical analysis and combine it with the literature review to form a final conclusion. It will further discuss the limitations of this study as well as make recommendations for future research. The following section will discuss the limitations of each country's reporting requirements as derived from the literature review.

4.2 Risk disclosure in the banking sector
For South African banks, integrated reporting is a governing tool that is required by the JSE as specified by their listing requirements (JSE, 2017). There is no specific disclosure requirements for integrated reporting, just merely a framework that can be used as a guideline (IIRC, 2012). The framework is aimed to assist with the creation of value by disclosing relevant information that is beneficial to all relevant organisations and stakeholders. It further gives guidelines as to how this information should look to derive value from it. However, as this is just a framework, banks will provide information in a manner that is most beneficial to them.

China's banks are required to report on risks as per IFRS requirements. They have to disclose information related to exposure and evaluation of credit risk, operational risk, market risk and any other relevant risks, as well as how the risk was managed (CASC, 2018). Cyber risk, or information technology risk as it is referred to by some banks, forms part of their operational risk portfolio. There is also a framework for IFRS, and as with the IRRC framework, this is merely a guideline and not necessarily implemented by the banks in China.

Both South Africa and China do have legislation and cyber risk reporting policies in place that falls outside of the IFRS and King IV requirements. However, these legislation and policies, the POPIA and the Chinese Cyber security Law, are fairly new and thus not fully implemented (Ning & Wu, 2019; Sophos, 2019). Furthermore, there is no specific framework for cyber risk reporting used by China's banks. Their annual reports show that this is incorporated in their main risk policy documentation.

4.3 Disclosure index summary

4.3.1 General information results

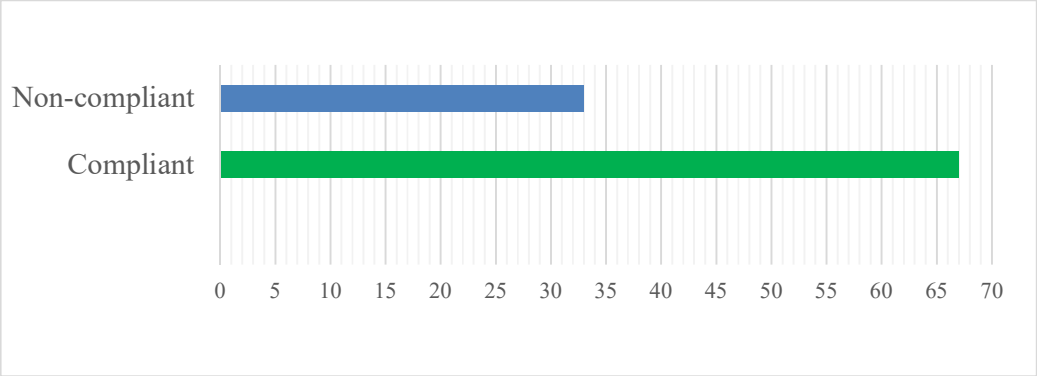
The general information sub section shows the distinct differences between the reporting methods of both countries. As shown in Table 3.2, all the South African banks produce integrated reports which equates to 50% of the total sample. King VI is also only a South African reporting requirement, thus also only equates to 50% of the total sample. Both South Africa and China must comply with IFRS, thus 100% of all the banks chosen for this sample have to comply with IFRS, further to this both countries are also subject to reporting all risk incidents.

4.3.2 Governance risk analysis summary

The initial steps in cyber risk management is to realise the current threats and set risk management goals (Eling & Schnell, 2016:480). Risk management has advanced to such a degree that there is a multitude of international and industrial standards (ISO/IEC 2700X) that can assist in managing cyber risk. A total of six governance related questions, focusing on risk reporting, cyber risk reporting and policies were derived from these frameworks and were utilised in building the disclosure index. As shown in Table 3.3, it was found that all the banks in the sample have policies in place regarding risk reporting, but as can be seen in Table 3.1 only three of the South African banks specifically indicate that they have cyber risk policies in place. This means that only 38% of the total sample have a cyber risk policy. The findings also show that all the relevant banking boards have taken ownership as they have assigned individuals who monitor risks in general. Seven out of the eight banks state that they have strategies in place to manage cyber risk, which is 88% of the total sample, however, the banks in China chosen for this study classifies cyber risk under their operational risk portfolio and just refers to risk management strategies in general. Only one bank, Agricultural Bank of China, did not make any mention of having such a strategy. This indicates that 100% of the South African banks have strategies in place to manage cyber risk, whereas only 75% of the Chinese banks have such strategies in place. Only 38% of the banks clearly defined cyber risk, That is three out of the total sample complied with this requirement. Table 3.1 shows that these three banks are all South African based. It is clear that 75% of South African banks define cyber risk and none of the banks in China define cyber risk. Of the eight banks only three of the South Africa banks identified cyber risk as a material item, which is 38% out of the total sample.

Looking at the total sample and shown in Graph 4.1, there was a 67% compliance rate. That means that the banks chosen for this sample complied with 67% of the governance questions

asked. However, when looking at the countries individually, China only had a 46% compliance rate where South Africa had almost double that at 88% compliance as seen in Graph 3.6. Furthermore, only Absa and Nedbank had complied with all the questions.



Graph 4.1 Group governance compliance rate

4.3.3 Cyber risk ranking summary

From Table 3.1 it is evident that only 2 banks provided risk rankings. That is 25% of the total sample size, all of which were South African banks. Absa ranked cyber risk as their number one risk that they face, and Nedbank ranked cyber risk as their second most critical risk. The other 62% of the sample did not rate cyber risk.

4.3.4 Cyber risk incidents summary

One of the SEC guidelines is that organisations disclose all prior cyber risk incidents and the impact thereof (Newman & Belknap, 2019). A study done by Li and Wang (2018) shows that organisations that follow this guideline are more likely to experience further cyber-attacks after making such information public. There is a supporting theory that shows cyber incidents could lead to enormous financial losses. The World Economic Forum (2015) stated in the extreme event, that internet connections across the world goes down, the financial impact within the first few days is estimated to be around $ 250 billion. In a study done by Hovav & D'Arcy (2003) results show that there is a negative share price effect for organisations, such as banks, that have a business model that is heavily reliant on the internet when they fall victim to cyber incidents. From all the banks sampled, there was a not a single cyber risk incident disclosed for the 2018 financial year. This could be due to no cyber-attacks taking place during the 2018 financial year or that organisations are reluctant to disclose this information out of fear of possible attacks even though regulators require it.

4.3.5 Mitigating procedures summary

Eling and Schnell (2016) states that to actively manage cyber risk, risk mitigation is a lot more plausible than risk avoidance. Risk mitigation along with the support of various instruments (e.g. anti-virus and firewalls) has proven to be most effective in reducing the probability of occurrence and minimising the size of losses. 100% of the banks showed that they had risk mitigation procedures in place.

The following section will summarise the findings from the disclosure index.

4.4 Summary

When combining the findings from the disclosure index we found that the reporting methods implemented by the two countries differs and governance reporting, within the respective countries, are the same. South African banks adheres to both IIRC and IFRS reporting requirements, whereas China adheres only to IFRS reporting requirements. Findings also indicated that all banks have general risk mitigation procedures in place. South African banks specifically refer to cyber risk mitigation procedures.

Cyber security is a key factor in banking operations as a result of digital technology advancements. The annual reports of China's banks classify risks under different categories. Cyber risk and information technology risk is classified as operational risks. As a result, China does not specifically refer to cyber risk but only ever discloses it as an operational risk in their annual reports. No ranking is associated with any of their risks or categories. This is in contrast when compared to the South African annual reports as South African banks clearly define cyber risk and not only rank it amongst their top risks but also recognises it as a material item. From a South African reporting perspective, cyber security is one of the greatest risks in the banking sector as it is specifically defined and referred to in their annual reports but the way in which it should be reported must be beneficial to stakeholders as it should reflect as a value add seeing that this is an IIRC requirement. Thus, for the stakeholders, it would be easier to assess the impact of cyber security from South Africa's reporting as it is more specific and should represent the value add.

For the 2018 financial year, there was no reported cyber risk incidents in either country. For China, however, as per Chinese Cyber security Law, if any cyber-attack poses a risk to national security, such an incident will not be published. This could mean that if there was an incident,

the banks could have been prohibited from reporting it to anyone except the relevant authorities.

From the disclosure index it is shown that South Africa's banks provides more defined and relevant cyber risk information. As conclusion, integrated reports published by South African banks are of a higher quality when compared to China's banks' annual reports.

4.5 Limitations

The chosen sample size only consists of the four largest banks from both countries. The assumption was made that these banks would represent the total population from their respective countries. Expanding the sample size could yield different results.

Since the legislation regarding cyber risk and cyber risk reporting is fairly new for both countries, there are many loopholes that organisations can exploit to mask their cyber incidents and report it in a manner that best suites them as it is negatively associated with an organisations good standing. This may also impact the accuracy of the reported information.

The study was compiled by extracting information from the organisations' annual reports only. Some organisations, such as Standard Bank provides separate reports, covering specific risk and policy associated topics which is not included in the annual reports and was therefore not considered.

4.6 Areas for further studies:

- Recreate the comparison of risk disclosure study in the banking sector between South Africa and China with a lager sample size.
- Do a full cyber risk policy study between the respective countries once it has been fully implemented.
- Do a risk comparative study of the banking sector in other countries utilising integrated reporting.
- Investigate technological advancement in the banking sector and the associated effects on cyber risk.

References

A4S. 2019. A4S aims. Available at: https://www.accountingforsustainability.org/en/about-us/overview.html (accessed on 25 April 2019).

Abdullah, W.A.W., Percy, M. & Stewart, J. 2015. Determinants of voluntary corporate governance disclosure: Evidence from Islamic banks in the Southeast Asian and the Gulf Cooperation Council regions. *Journal of Contemporary Accounting & Economics*, 11(3):262-279.

Abu El Ata, N. & Schmandt, R. 2016. *The tyranny of uncertainty : a new framework to predict, remediate and monitor risk*. Heidelberg: Springer Science and Business Media.

Al-Hadi, A., Hasan, M.M. & Habib, A. 2016. Risk committee, firm life cycle, and market risk disclosures. *Corporate Governance: An International Review*, 24(2):145-170.

Amery, P. 2012. Shortened Settlement Threatens ETF Liquidity. Available at: https://www.etf.com/sections/features/11255-shortened-settlement-threatens-etf-liquidity.html?nopaging=1 (accessed 25 September 2019).

Amran, A., Manaf Rosli Bin, A. & Che Haat Mohd Hassan, B. 2009. Risk reporting: An exploratory study on risk management disclosure in Malaysian annual reports. *Managerial Auditing Journal*, 24(1):39-57.

Asongu, S., Akpan, U.S. & Isihak, S.R. 2018. Determinants of foreign direct investment in fast-growing economies: evidence from the BRICS and MINT countries. *Financial Innovation*, 4(1).

Bengtsson, M. 2016. How to plan and perform a qualitative study using content analysis. *NursingPlus Open*, 2:8-14.

Bernardi, L., Keim, S. & Von der Lippe, H. 2007. Social influences on fertility: A comparative mixed methods study in Eastern and Western Germany. *Journal of mixed methods research*, 1(1):23-47.

Berry, C. 2018. Cyberattacks targeting South Africa: expensive lessons to be learnt Available at: https://www.camargueum.co.za/post/cyberattacks-targeting-south-africa-expensive-lessons-to-be-learnt (accessed 11 November 2019).

BIS. 2013. Principles for effective risk data aggregation and risk reporting. Available at: https://www.bis.org/publ/bcbs239.pdf (accessed 3 June 2020).

Bouveret, A. 2018. Cyber risk for the financial sector: a framework for quantitative assessment: International Monetary Fund.

Bowen, G. 2009. Document Analysis as a Qualitative Research Method. *Qualitative Research Journal*, 9:27-40.

Bragg, S. 2018. Financial statements. Available at: https://www.accountingtools.com/articles/2017/5/10/financial-statements (accessed 17 November 2019).

Bryman, A. & Bell, E. 2014. *Research methodology: business and management contexts*. Cape Town: Oxford University Press Southern Africa.

Businesstech. 2017. Battle of the banks: how SA's big five banks compare. Available at: https://businesstech.co.za/news/banking/182873/battle-of-the-banks-how-sas-big-five-banks-compare/ (accessed 25 July 2018).

Businesstech. 2018. These are South Africa's biggest banks. Availabel at: https://businesstech.co.za/news/banking/245061/these-are-south-africas-biggest-banks/ (accessed 5 October 2019).

Businesstech. 2019. These are the 10 biggest overall risks for South Africa. Available at: https://businesstech.co.za/news/business/337839/these-are-the-10-biggest-overall-risks-for-south-africa/ (accessed 10 November 2019).

Cantoria, C. 2019. Risk Mitigation Strategies and Risk Mitigation Plan: Tips for Documentation & Implementation in Project Management. Available at: https://www.brighthubpm.com/risk-management/47934-risk-mitigation-strategies-and-risk-mitigation-plan/) (accessed 10 November 2019).

Carels, C.M. 2014. Integrating reporting: an analysis of the extent of social environmental and ethical matters in corporate reporting.

CASC. 2018. China Accounting Standards Committee. Available at: http://www.casc.org.cn/2015/1123/123195.shtml (accessed 28 July 2018).

chinaplus.cri.cn. 2018. China holds top four rankings in list of world's largest banks. Available at: http://en.ce.cn/Business/topnews/201807/05/t20180705_29633951.shtml (accessed 28 July 2018).

Choudhury, F. 2014. Making Financial Reporting Better: Strengthening the Financial Reporting Supply Chain. Avaiable at: https://www.ifac.org/knowledge-gateway/business-reporting/discussion/making-financial-reporting-better-strengthening (accessed 17 November 2019).

CIMA. 2008. Introduction to managing risk. Available at: https://www.cimaglobal.com/Documents/ImportedDocuments/cid_tg_intro_to_managing_rist.apr07.pdf (accessed 17 February 2020).

Cloudflare. 2019. What is a DDoS Attack? Available at: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ (accessed 10 November 2019).

Craddock, J. & West, J. 2018. Wells Fargo Circles the Wagons: Communicating During a Crisis.

Crowther, D. 2018. A Social Critique of Corporate Reporting: A Semiotic Analysis of Corporate Financial and Environmental Reporting.

Cruickshank, C. 2019. Beware the evolving beast: cybersecurity in financial services. Available at: https://www.ocorian.com/article/beware-evolving-beast-cybersecurity-financial-services (accessed 11 September 2019).

Deloach. 2019. 10 Top Risks for 2019. Available at: https://www.corporatecomplianceinsights.com/10-top-risks-for-2019/ (accessed 2 October 2019).

Deloitte. 2012. Core beliefs and culture Chairman's survey findings. Available at: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/gx-core-beliefs-and-culture.pdf (accessed 9 September 2019).

Demrovsky, C. 2019. Don't Ignore These 10 Global Business Risks In 2019. Available at: https://www.forbes.com/sites/chloedemrovsky/2019/01/14/dont-ignore-these-10-global-business-risks-in-2019/#3ecbaba914c0 (accessed 10 November 2019).

Dietz, T., Börner, J., Förster, J.J. & Von Braun, J. 2018. Governance of the bioeconomy: A global comparative study of national bioeconomy strategies. *Sustainability*, 10(9):3190.

Eling, M. & Schnell, W. 2016. What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance*, 17(5): 474-491.

Eling, M. & Wirfs, J.H. 2016. Cyber Risk: Too Big to Insure?: Risk Transfer Options for a Mercurial Risk Class. Institute of Insurance Economics I. VW-HSG.

Elshandidy, T. & Neri, L. 2015. Corporate Governance, Risk Disclosure Practices, and Market Liquidity: Comparative Evidence from the UK and I taly. *Corporate Governance: An International Review*, 23(4):331-356.

Elshandidy, T., Shrives, P.J., Bamber, M. & Abraham, S. 2018. Risk reporting: A review of the literature and implications for future research. *Journal of Accounting Literature*, 40:54-82.

Epstein, M.J. & Rejc, A. 2006. *The reporting of organizational risks for internal and external decision making*. CMA, Canada.

Fleming, S. 2019. The top 10 risks to the global economy, according to the Economist Intelligence Unit. Available at: https://www.weforum.org/agenda/2019/03/the-top-10-risks-to-the-global-economy-according-to-the-economists-intelligence-unit/ (accessed 10 November 2019).

Flower, J. 2015. The International Integrated Reporting Council: A story of failure. *Critical Perspectives on Accounting*, 27:1-17.

Forum, W.E. 2015. Global Risk. *Insight Report. 10th Edition.* Available at: http://www3. weforum. org/docs/WEF_Global_Risks_2015_Report15. pdf. (accessed 1 July 2020).

FRC. 2017. Risk and viability reporting. Avialable at: https://integratedreporting.org/wp-content/uploads/2017/11/FRBRisk-and-Viability-Reporting.pdf (accessed 5 October 2019).

Glazer, E. 2016a. How Wells Fargo's High-Pressure Sales Culture Spiraled Out of Control. *The Wall Street Journal*, 16.

Glazer, E. 2016b. Wells Maps a Crisis Plan— Executives Say Bank's Situation Will Get Harder Before It Gets Better After Scandal. *The Wall Street Journal*, C1, C2.

Greenwald, J. 2011. Rogue trader case shows serious risk management flaws. Available at: https://www.businessinsurance.com/article/20111002/NEWS07/310029982 (accessed 26 September 2019).

GRI. 2018. About Sustainability Reporting. Available at: https://globalreporting.org/information/sustainability-reporting/Pages/default.aspx (accessed 30 September 2018).

GRI. 2019. About GRI. Available at: https://www.globalreporting.org/information/about-gri/Pages/default.aspx (accessed 25 April 2019).

Hackston, D. & Milne, M.J. 1996. Some determinants of social and environmental disclosures in New Zealand companies. *Accounting, auditing & accountability journal*. 9(1): 77-108

Härle, P., Havas, A., Kremer, A., Rona, D.H.S. 2016. *The future of bank risk management*. Available at: https://www.mckinsey.com/business-functions/risk/our-insights/the-future-of-bank-risk-management# (accessed 26 January 2020).

Harris, R. 2013. Warning Signs Prior to the Financial Crisis of 2008: A Comparative Analysis. *Journal of Management & Engineering Integration*, 6(1):88-97.

Hovav, A. & D'Arcy, J. 2003. The impact of denial-of-service attack announcements on the market value of firms. *Risk Management and Insurance Review*, 6(2):97-121.

Humphrey, C., O'Dwyer, B. & Unerman, J. 2017. Re-theorizing the configuration of organizational fields: the IIRC and the pursuit of 'Enlightened' corporate reporting. *Accounting and Business Research*, 47(1):30-63.

IFRS. 2018. List of IFRS Standards. Available at: https://www.ifrs.org/issued-standards/list-of-standards/ (accessed 25 July 2018).

IIRC. 2012. Draft Framework Outline. Available at: http://integratedreporting.org/news/draft-framework-outline/ (accessed 27 April 2019).

IIRC. 2015. The International <IR> Framework.

IIRC. 2018. Why? The need for change. Available at: http://integratedreporting.org/why-the-need-for-change/ (accessed 2 October 2018).

IODSA. 2010. *King Report on Governance for South Africa 2009 ; King Code of Governance Principles for South Africa 2009 ; Companies Act 71 of 2008*. Cape Town: Jutalaw.

IODSA. 2016. King IV Report.

IRCSA. 2013. The International Integrated Reporting Framework.

Johnson, R.B. & Onwuegbuzie, A.J. 2004. Mixed methods research: A research paradigm whose time has come. *Educational researcher*, 33(7):14-26.

JSE. 2017. JSE Limited Listings Requirements.

Kaffenberger, L. & Kopp, E. 2019. Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment. Available at: http://carnegieendowment.org/files/Kaffenberger_Cyber_Risk_Scenarios_final1.pdf (accessed 3 February 2020).

Khlif, H., Ahmed, K. & Souissi, M. 2017. Ownership structure and voluntary disclosure: A synthesis of empirical studies. *Australian Journal of Management*, 42(3):376-403.

Khlif, H. & Hussainey, K. 2016. The association between risk disclosure and firm characteristics: a meta-analysis. *Journal of Risk Research*, 19(2):181-211.

Koshy, Y. 2018. When the world almost ended. *New Internationalist*, 514:12.

KPMG. 2016. King IV Summary Guide.

KPMG. 2017. Overview of China's Cybersecurity Law.

Krzus, M.P. 2011. Integrated reporting: if not now, when. *Zeitschrift für internationale Rechnungslegung*, 6:271-276.

Lashinsky, A. 2017. Riders on the Storm. *FORTUNE*, 159(9):72.

Lee, P. 2011. UBS rogue trader Kweku Abodoli exploited ETF settlement loophole. Available at: https://www.euromoney.com/article/b12kjcmn0vm3ht/ubs-rogue-trader-kweku-abodoli-exploited-etf-settlement-loophole (accessed 25 September 2019).

Li, H., No, W.G. & Wang, T. 2018. SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, 30:40-55.

Linsley, P. & Shrives, P. 2000. Risk management and reporting risk in the UK. *Journal of Risk*, 3:115-129.

Linsley, P.M. & Shrives, P.J. 2006. Risk reporting: A study of risk disclosures in the annual reports of UK companies. *The British Accounting Review*, 38(4):387-404.

McDonald, C. 2013. Lehman Couldn't Handle the Risk Management Truth. Available at: https://www.cfo.com/risk-management/2013/02/lehman-couldnt-handle-the-risk-management-truth/ (accessed 25 September 2019).

Mzekandaba, S. 2019. IOT devices are attacked within five minutes of being connected. Available at: https://www.itweb.co.za/content/nWJadMb89N4vbjO1 (accessed 10 November 2019).

Newman, C. & Belknap, P. 2019. SEC Cyber Briefing: Regulatory Expectations for 2019. Available at: https://corpgov.law.harvard.edu/2019/01/02/sec-cyber-briefing-regulatory-expectations-for-2019/ (accessed 17 July 2020).

Ning, S. & Wu, H. 2019. China: Cybersecurity 2020. Available at: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/china (accessed 17 November 2019).

Norton. 2019a. What is a data breach? Available at: https://us.norton.com/internetsecurity-privacy-data-breaches-what-you-need-to-know.html (accessed 10 November 2019).

Norton. 2019b. What is a distributed denial of service attack (DDoS) and what can you do about them? Available at: https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html (accessed 10 November 2019).

Norton. 2019c. What is a man-in-the-middle attack? Available at: https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html (accessed 10 November 2019).

Norton. 2019d. What is a Trojan? Is it a virus or is it malware? Available at: https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html (accessed 10 November 2019).

Norton. 2019e. What is mobile ransomware? Available at: https://us.norton.com/internetsecurity-mobile-what-is-mobile-ransomware.html (accessed 10 November 2019).

Norton. 2019f. What is phishing? Available at: https://us.norton.com/internetsecurity-online-scams-what-is-phishing.html (accessed 10 November 2019).

Norton. 2019g. What is spear phishing? Available at: https://us.norton.com/internetsecurity-malware-what-spear-phishing.html (accessed 10 November 2019).

Oliveira, J., Rodrigues, L.L. & Craig, R. 2013. Company Risk-related Disclosures in a Code Law Country: A Synopsis. *Australasian Accounting, Business and Finance Journal*, 7(1):123-130.

Östlund, U., Kidd, L., Wengström, Y. & Rowa-Dewar, N. 2011. Combining qualitative and quantitative research within mixed method research designs: a methodological review. *International journal of nursing studies*, 48(3):369-383.

Oxford. 2019. Definition Available at: https://www.oxfordlearnersdictionaries.com/definition/english/definition?q=definition (accessed 10 November 2019).

Pourkhomami, P. 2018. IT Security Policies: Why Every Organization Must Have Them. Available at: https://www.osibeyond.com/resources/it-security-policies-every-organization-must-have-them/ (accessed 10 Novmber 2019).

Regan, J. 2019. What is Malware? How Malware Works & How to Remove It. Avaiable at: https://www.avg.com/en/signal/what-is-malware (accessed 10 November 2019).

Riff, D., Lacy, S., Fico, F. & Watson, B. 2019. *Analyzing media messages: Using quantitative content analysis in research*.

Rossi, F., Orelli, R. 2019. Investigating New Reporting Practices in Local Government: Is Integrating Reporting the Best Way? *Qualitative Research in Intangibles, Intellectual Capital and Integrated Reporting Practices.*

SABRIC. 2019. Digital Banking Crime Statistics. Available at: https://www.sabric.co.za/media-and-news/press-releases/digital-banking-crime-statistics/ (accessed 11 November 2019).

SARB. 2012. Regulations Relating to Banks. *35950*.

SARB. 2019. Directiver 2/2019. 15/8/1/3.

Sargsyan, G. 2018. Effect of statutory and regulatory protection in investment decision. Universidad de Alicante.

SEC. 2012. Proxy Disclosure Enhancements. Available at: https://www.sec.gov/rules/final/2009/33-9089-secg.htm (accessed 10 November 2019).

Securities & Commission, E. 2018. Commission Statement and Guidance on Public Company Cybersecurity Disclosures. *February*, 26:2018.

Setia, N., Abhayawansa, S., Joshi, M. & Huynh, A.V. 2015. Integrated reporting in South Africa: some initial evidence. *Sustainability Accounting, Management and Policy Journal*, 6(3):397-424.

Sophos. 2019. Only 34% of South African organisations ready to comply with POPI Act. Available at: https://www.itweb.co.za/content/nWJadvb8z3bMbjO1 (accessed 11 November 2019).

Sovern, J. 2017. Free-market failure: The Wells Fargo arbitration clause example. *Rutgers UL Rev.*, 70:417.

Stubbs, W. & Higgins, C. 2018. Stakeholders' perspectives on the role of regulatory reform in integrated reporting. *Journal of Business Ethics*, 147(3):489-508.

Tashakkori, A. & Creswell, J.W. 2007. *The new era of mixed methods*.

Tayan, B. 2019. The Wells Fargo cross-selling scandal. *Rock Center for Corporate Governance at Stanford University Closer Look Series: Topics, Issues and Controversies in Corporate Governance No. CGRP-62 Version*, 2:17-11.

TGE. 2019. China: Listed companies. Available at: https://www.theglobaleconomy.com/China/Listed_companies/ (accessed 19 October 2019).

Thomasson, E. 2011. How a rogue trader crashed UBS. Available at: https://mg.co.za/article/2011-09-27-how-a-rogue-trader-crashed-ubs (accessed 26 September 2019).

Thun, T. 2015. European Banks Underestimate the Challenges of BCBS 239 Implementation.

Tylor, H. 2018. What Are Cyber Threats: How They Affect You and What to Do About Them. Available at: https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/ (accessed 17 November 2019).

Vieru, K. 2017. The time is right for Integrated Reporting. Available at: http://integratedreporting.org/news/the-time-is-right-for-integrated-reporting/ (accessed 2 April 2018).

Wang, Z., Chen, J. & Zhao, X. 2018. Risk Information Disclosure and Bank Soundness: Does Regulation Matter? Evidence from China. *International Review of Finance*, n/a(n/a).

Warren, P., Kaivanto, K. & Prince, D. 2018. Could a cyber attack cause a systemic impact in the financial sector? *Bank of England Quarterly Bulletin*, 58(4):21-30.

Whitfield, G. 2012. The Importance of Proper Definition. Available at: https://piadvice.wordpress.com/2012/06/13/the-importance-of-proper-definition/ (accessed 10 November 2019).

Wilson, H. 2014. UBS banker banned over $2.3bn rogue trading scandal.

Appendix A

- https://www.jse.co.za/current-companies/companies-and-financial-instruments.