The Role of Information Technology in the Risk Management of Businesses in South Africa

B Schutte

Lecturer
Department of Accountancy
University of Johannesburg
South Africa

B Marx

Professor, Head of Auditing and Head of Department
Department of Accountancy
University of Johannesburg
South Africa

Abstract

Information Technology is a dynamic and constantly evolving field which has dramatically changed the way in which businesses operate. Organisations now have to ensure that information technology is incorporated into their risk management processes and the strategies to mitigate those risks.

This study investigated the role of information technology in risk management processes, focusing on the type of information technology risks and threats that affect organisations. An empirical study of the integrated reports of the top 40 companies listed on the Johannesburg Securities Exchange was conducted to investigate the information technology risk management disclosure practices. The study was completed in 2016, before the King IV Code of Corporate Governance for South Africa became effective and accordingly, focused only on the King III principles of information technology governance and risk management.

The study found that companies are mitigating information technology risks and have included information technology into their risk management processes. The results also revealed that awareness of information technology risk may be industry-driven, as companies operating in information technology environments were more likely to be exposed to information technology risk.

Key words**:** Information technology, risk management, risk management of IT, IT risks, IT governance.

1. INTRODUCTION

Information Technology (hereafter IT) has dramatically changed the way in which businesses operate as today, the majority of organisations rely on electronic information systems to perform, record and report financial information. The changes in IT pose significant challenges to organisations, which need to ensure that their IT systems are managed correctly and are incorporated into the risk management processes of the organisation. The *Investor's Business Daily* (2014:1) reported that a global business risk study performed by PricewaterhouseCoopers (hereafter PWC) indicates that 58% of executives and risk managers identified technological change and IT risk as a key concern. The importance of IT for organisations is emphasised by Wessels and Steenkamp (2007:114) who observe that businesses engage in increasingly complex arrangements and transactions.

IT is widely regarded as one of the key drivers changing the business environment and is integrated into almost all aspects of business. The pivotal role of IT in organisations is emphasised by Patterson (2015:2), who states that the majority of entities these days would concur that they are completely dependent on IT for their continued success.

The new era of IT and IT systems has made the environment in which organisations operate particularly challenging. New technologies are constantly evolving and organisations need to keep abreast of these changes (Abdolghassem, Mehdi, Hessam, Alireza, Amirhesam and Simin Seifi, 2013:1). Optimal Networks (2017) reports that organisations started to increase their IT budgets in 2014, while Gartner, the world's leading IT research and advisory company, observed a 2.1% increase in overall global IT spending from 2013 onwards (Optimal Networks, 2017).

According to the IT Governance Institute (2007:9), organisations that wish to make use of the benefits that IT has to offer also need to understand the risks associated with IT. As a result, organisations need to find ways of aligning their IT strategy with their business strategy. This would assure internal and external stakeholders that mitigating IT risk is an important aspect of business operations and demonstrate that

an effective relationship and communication exist between the business and IT (IT Governance Institute, 2007:9).

The next section will discuss the objectives and scope of the study, followed by the theoretical background, research methodology, findings and interpretations, areas for future research and conclusion.

2. BACKGROUND

The objective of this paper is to add to the existing body of knowledge by obtaining a thorough understanding, from existing literature and empirical evidence, of the:

- Concepts of the governance of IT and risks to ensure organisations understand their importance;
- Role of IT within an organisation to ensure that organisations are fully aware of what IT entails;
- Concept of risk management within the organisation to ensure that organisations are aware of what risk management is and whether their risk management processes are effective in addressing IT risks; and
- Pivotal role of IT within the risk management processes of an organisation to ensure that organisations are benefitting fully from IT systems.

The above objectives are achieved through a literature review and an empirical study consisting of content analysis of the integrated reports of the top 40 listed companies on the Johannesburg Stock Exchange (hereafter JSE) for the disclosure of IT risks and IT risk management.

2.1 IT and risk management

IT and risk management are two key components that should be incorporated into the processes and governance structures of organisations. Accordingly, the board of directors (hereafter BOD) should set the tone at the top, and the Chief Financial Officer (hereafter CFO) and Chief Information Officer (hereafter CIO) should fully understand not only the opportunities of IT, but also the potential limitations of IT risk (Anand, 2010:57).

Constant advances in technology pose one of the biggest risks to IT. Marx (2008:82) maintains that the development of IT, electronic commerce and the increased reliance on IT resources have exposed modern business to numerous challenges and significant new risks. Wessels (2006:131) concurs, stating that South African businesses operate in an environment that is changing rapidly. The changes in the IT landscape create a new dimension for entities, bringing both opportunities and challenges. IT plays a vital role in entities today and is a critical factor in responding to increasingly globalised markets (Mohamad, Ramayah & Lo, 2017). Madslien (2017) supports this view, noting that the advances in IT create new opportunities for entities.

FNR Solutions Inc. (2016:1) reports that IT has enabled an organisation's finance function to compete globally because, for example, a person's credit score and credit ratings are currently available securely online. It is clear that IT is an increasingly critical part of an organisation and that it is crucial for organisations to thoroughly understand the role played by IT within the organisation to ensure that risk management processes address IT sufficiently.

Organisations may not always be fully aware of all the IT risks that they could be exposed to since such risks may not always be easily identifiable due to their complexity and ever-changing nature. Ernst and Young (2013:4) note that many organisations find it challenging to identify and manage risks that are associated with emerging technologies. In their fifteenth annual Global Information Security Survey, Ernst and Young reported that organisations which are striving to close the gap created by mobile computing, social media and cloud and cyber-attacks, must consider transforming their approach to identifying IT risks.

Organisations specifically trading in the accounting and consulting sectors have major concerns regarding IT risk management and the compliance that comes with it. Businesses which do not always understand or have not yet considered all the risks related to IT may not be adequately prepared to mitigate those risks. As a result, they may be vulnerable to the challenges and demands associated with their IT environment (Woodard, 2013:1).

Alongside the benefits that IT has to offer, organisations will also be exposed to new risks and threats such as cyber security, hacking and business continuity challenges, to name a few. Risk management therefore plays a critical role in protecting information (Tohidi, 2001:881). Tohidi (2011:881) adds that effective risk management is vital element in an IT-driven organisation. Hopkin (2017) agrees that having a risk management process is key to enhancing the effectiveness and efficiency of all operations and business processes. Since organisations rely on IT and use information systems to process their information, it is of the utmost importance to understand the IT risks that organisations are exposed to.

2.2 IT risks

IT risks can be defined as the probability that a certain threat will trigger or intentionally exploit a vulnerability in the information systems and have a significant effect on the organisation (National Institute of Standards and Technology (hereafter NIST), 2015:1). According to NIST (2015:1), IT risks arise from:

- Unauthorised disclosure, changes or the destruction of information;
- Unintentional errors and omissions;
- IT-related disruptions, whether accidental or as a result of human error; and
- Lack of due care and diligence exercised in the implementation and operation of the information systems.

Organisations need to ensure complete awareness of what these types of IT risks are to confirm that these risks are addressed in their risk management process. IBM Global Technology Services (2011:3–4) echo that IT risks can involve a range of threats that can be divided into three categories, namely, data-driven, business-driven and event-driven threats. Data-driven threats receive the most attention because they are likely to occur more frequently. Data-driven threats include but are not limited to the following: viruses, worms, data corruption, disk failure and network problems. Business-driven threats will directly affect the business continuity and operations and will receive specific attention form the BOD. For example, business-driven threats include system availability failures, application outage and workplace inaccessibility. Event-driven threats will disrupt the workforce, the processes, applications, data and

infrastructure of the organisation. Examples of event-driven threats are failure to meet industry standards, political events, natural disasters and power failures.

Traci Mizoguchi, the Enterprise Risk Services Senior Manager at Deloitte and Touche identified the top emerging IT risks based on observations of the marketplace (Mizoguchi, 2012:4–13). The top IT related risks as identified according to Mizoguchi are:

Social networking – the use of social networking is constantly emerging and changing. It is important for organisations to ensure that they are aware of social networking platforms and to monitor these platforms to ensure that they protect the reputation of the organisation and constantly show that they are committed to their clients by responding to claims of bad service.

Mobile devices – with the rapid expansion in mobile devices, organisations must constantly monitor devices that connect to the company servers and Wi-Fi to ensure that there is no unauthorised access to vital data or loss or release of critical business data.

Malware – as IT becomes more complex and sophisticated, so does malware. IT criminals are becoming smarter and try out new ways to inflict harm on the users of IT. Organisations will have to be even more conscious about threats such as malware and make sure these types of threats are monitored.

Corporate espionage – this relates to organisations experiencing specific, targeted efforts to gain an advantage, assisted by improved mobile computing technologies that increase access to various kinds of information.

IT governance – one of the biggest risks for organisations is the failure to apply the principles of IT governance as set out in the King Code on Corporate Governance and thus run the risk of tarnishing the reputation of the organisation. For organisations listed on the JSE, this could mean losing investor and stakeholder confidence and their listing on the JSE.

Electronic records management – as organisations increasingly use electronic records management, the risks regarding the use of such systems are growing. The major risks that organisations will now have to focus on will be the loss of data in the

conversion process to electronic records management systems and the storage and retention of data on these systems to ensure that the data is protected.

Data management – with the increased regulatory requirements to ensure that data is well-managed and secure, such as the South African Protection of Personal Information Act, organisations will have to ensure that they have measures in place to identify any threat to data and have ways to mitigate these risks.

Cloud computing – with organisations now having the option to make use of cloud computing and storing their data on the cloud, it is very important that the following risks associated with cloud computing are understood:

- Lack of internet access, which means that organisations will not be able to access their data; and
- Increased reliance on third parties to run their IT, which places critical business data at risk of being stolen.

During the regulatory and risk management indicator survey conducted by Wolters Kluwer Financial Services in June 2013, it was evident that organisations are under increased regulatory and risk management pressure regarding their IT risks and mitigating compliance than ever before (Woodard, 2013:1). The results from this survey showed that the greatest risk concern among financial professionals was regulatory risk at 56%, fraud at 33%, asset and liability management at 28% and IT risk at 25% (Woodard, 2013:1). It can be seen that IT risk is the fourth highest risk management concern, according to the regulatory risk management indicator. These figures reflect the importance for organisations to have a thorough understanding of IT-related risks. It is not only important for organisations to understand IT risks, but also what can be done to ensure that exposure to IT risks is effectively managed.

The emerging world of the internet, e-commerce, on-line trading and electronic communications have forced organisations to conduct their business electronically. This, in turn, has resulted in new risks that must be well governed and controlled (Institute of Directors, 2009:14–15).

2.3 The governance of risks and IT

In organisations, the reliance on IT has become a crucial part of the growth, sustainability and support of the business. The omnipresence of technology in the operations of an organisation has created a critical reliance on IT which has, in turn, resulted in a specific focus on IT governance (De Haes and Van Grembergen (2008:1). Organisations may ask, "Why is IT governance such an important principle to apply?" The answer is simple: "The ultimate goal of IT governance is to achieve better alignment between [the organisation's] IT systems and [its] business" (De Haes and Van Grembergen, (2008:1). Lainhart (2000:33) emphasises that IT governance helps an organisation to achieve critical success factors through the effective and efficient deployment of reliable information and applied technology.

IT governance was included in the King III Code of Corporate Governance for South Africa in 2009 (hereafter King III), as information systems were becoming more prevalent. This pervasiveness of information systems has mandated the governance of IT as a corporate imperative (Institute of Directors, 2009:14–15).

The IT governance chapter in King III includes specific principles and recommendations that organisations can apply to ensure good IT governance. These principles and recommendations state that ultimately, the BOD will be responsible for IT governance and that IT governance must be a regular item on the agenda of the board to ensure that the organisation constantly practices good IT governance (Institute of Directors, 2009:39–41).

One key aspect of the recommendations in King III is that the board should establish an IT steering committee to assist with the governance of IT. The CEO of the organisation is required to appoint a CIO to manage the IT committee and IT governance within the organisation. The CIO should be a suitable and experienced person who is to interact with the board, appropriate committees and executive management (Institute of Directors, 2009:40). Since this study precedes the implementation of King IV in 2017, it focuses solely on the principles of IT governance in terms of King III.

King III has very specific principles and recommendations that organisations should apply in terms of the governance of risk. The BOD carries the overall responsibility of risk governance. Some of the BOD's other responsibilities in terms of the governance of risk include:

- Continual risk monitoring and assessments;
- Ensuring that management considers appropriate risk responses;
- Receiving assurance on the effectiveness of the risk management processes; and
- Ensuring that there are processes in place for complete, relevant, accurate, timely and accessible risk disclosure to management (Institute of Directors, 2009:35-39).

It is important for the BOD to appoint a risk committee to be responsible for the risk management policy and the planning and monitoring of the risk management process. The risk committee must appoint a Chief Risk Officer (hereafter CRO) who will report to the board, relevant committees and executive management on strategic matters regarding risks (Institute of Directors, 2009:35-37).

2.4 Risk management in an organisation

The risk management process of an organisation should be an integral part of its strategic management; the focus of good risk management should revolve around how the organisation identifies and treat risks. The overall objective of a risk management process will be to add the maximum sustainable value to all its activities across the organisation (FERMA, 2002:3).

Risk management should be a continuous and developing process throughout the whole organisation, focusing on the organisation's strategy and implementation. Risk management should be adopted into the culture of the organisation with a well-conceived plan led by senior management. Organisations should ensure that their risk management processes methodically address all the risks in their past, present and future activities (FERMA, 2002:3).

Since the risk management process focuses on all the risks affecting an organisation, it would be prudent to implement an IT risk management framework to ensure that IT risks are incorporated into the process. This framework should be based on a set of guiding principles (Information Systems Audit and Control Association (hereafter ISACA) 2015:2) and have a range of benefits or success factors. Ernst and Young (2013:6) suggest that these success factors should:

- Focus on the organisation's corporate strategy while assessing the IT risk landscape;
- Include new IT risks resulting from emerging technologies and regulatory requirements;
- Define key IT risk indicators; and
- Integrate the IT risk management framework with enterprise risk management.

The alignment of the IT risk management framework to the strategic business initiatives of the organisation in the IT industry should:

Include a risk assessment to look for vulnerabilities and threats specifically relating to emerging technologies such as cloud computing, social media and mobile technologies;
Design policies and internal controls to ensure that IT risks are reduced to an acceptable level; and
Monitor override abuse through policies and procedures to ensure that management does not abuse its power to override systems (Woodard, 2013:2):

2.5 Role of IT in the risk management process

Regarding the risk management process, many organisations fall short when it comes to having skilled risk resources, analytical processes and tools. The performance of many risk management processes can improve if these processes were to incorporate better methods to identify, collect and analyse the risk data in order to prepare appropriate mitigation strategies (Patterson, 2015:1).

An effective risk management process starts with good data to provide the organisation with sound statistics on which to base informed decisions. To collect quality data, organisations will have to implement robust front-end systems, data architecture with limited human intervention, databases and business intelligence technology (Wilkinson, 2011:2). Data analysis can take various forms, however, actuarial techniques of modelling recognise that there is no single way to quantify risk. Wilkinson (2012:2) states, however, that the increase in computers or IT computing will make actuarial techniques of modelling far more effective and efficient.

2.6 Governance, risk management and compliance and the role of IT

Governance, risk and compliance can be described as a management tool to promote criteria unification, collaboration and communication between the organisation's different stakeholders in managerial positions (Adams, Ruiz and Rivera, 2013:4). Governance, risk and compliance can add value to organisations through the integration of administration and risk management, internal control and compliance.

The most important role of IT within the governance, risk and compliance process is that IT can streamline the integration of this process and make it more cost-effective (Anand, 2010:58). When the IT components in an organisation are properly aligned with the business strategies, IT can be used for value creation and competitive advantage (Anand, 2010:58). PwC (2017) support the above statement, concurring that IT governance, risk and compliance ensure that the activities and functions of the organisation will support the objectives, achieve the benefits it has to offer against the strategy, and manage critical IT resources effectively.

For the governance, risk and compliance process to be successful within an organisation, there should be consistent terminology and language. IT is crucial in this regard as it ensures that there is a common governance, risk and compliance repository and data model. This repository and data model will contain large amounts of data that will contain the governance, risk and compliance within an organisation (*IT Business Edge*, 2016:1). IT can create an automated governance, risk and compliance process that will save the organisation time and effort by reducing errors linked to manual processes (*IT Business Edge*, 2016: 1).

2.7 Enterprise risk management and the role of IT

Enterprise risk management (hereafter ERM) can be defined as:

> …a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, and to provide reasonable assurance regarding the achievement of entity objectives (Committee of Sponsoring Organisations (COSO) of The Treadway Commission, 2004:2).

An effective ERM programme should incorporate risk-informed and risk-aware decisions into the governance structures and processes of an organisation. For the ERM programme to be effective, it will continually have to provide management with the ability to capture, evaluate, analyse and respond to risks that arise from internal and external sources (Patterson, 2015:3).

A key component of an effective ERM programme is having timely information. For example, when an organisation is immediately aware that a key supplier has experienced significant disruptions in its raw materials supply chain, timely information can help the organisation compensate for this risk (Patterson, 2015:3). Since timely information is such a critical component, many organisations make use of IT to monitor social media platforms to collect timely information on customer services, product quality and service delivery issues (Patterson, 2015:3).

Many ERM systems contain an inventory listing of all the entity-wide risks with which the organisation is faced. However, from an IT perspective, these inventory listings can be managed better when using IT such as spreadsheets and tables. When the data contained in these inventory listings has to be extracted, IT has an important role to play in simplifying the process. Tools that can help the CIO to extract data are electronic data warehouses, business intelligence applications and information analytical technologies (Patterson, 2015:4).

IT can also assist an ERM system when it comes to risk analysis because there are some risks, such as a market-wide risk, geographical risk and economic changes, that may only be anticipated or felt when they are reported by management. Statistical modelling tools can help support an ERM system's risk analysis as they allow for risk

scenarios that are even more diverse, to be evaluated which results in better decision-making (Patterson, 2015:7).

For organisations which want effective ERM programmes, it is of the utmost importance to ensure that the risk management function and IT function work together to enhance or build ERM support systems. Organisations should also consider including IT executives as part of the risk committee and ensure that the ERM or risk management programme is part of the overall IT governance process of the organisation (Patterson, 2015:9).

3. RESEACH METHODOLOGY

The objective of this study was to identify the role of IT in the risk management process. To achieve this objective, a literature study was conducted to explore IT concepts and risk management and to identify the role of IT within the risk management process. The results of the literature study provide the basis for the empirical study, which takes the form of a content analysis of the integrated reports of the top 40 JSE-listed companies.

3.1 Population

The top 40 JSE-listed companies were selected to perform a content analysis of their 2015/2016 integrated reports. These companies were chosen because of their listing on the JSE, which represents the largest listed companies in South Africa and, accordingly, the largest 40 companies ranked by market capitalisation. The reason the 2015/2016 annual integrated reports were used is because not all companies had already issued 2016/2017 annual integrated reports at the time of the analysis. The top 40 listed companies are also likely to apply the best practices in terms of the governance of IT and risks.

3.2 Content analysis

A content analysis of the integrated reports of the top 40 JSE-listed companies was performed because an integrated report discloses the practices a company follows concerning IT and risk management. Integrated reports also reveal the top risks affecting a company. The questions on the content analysis control sheet were based

on the literature study and were designed to extract information easily from the integrated reports in order to answer the questions. The findings of the content analysis do not reflect the findings of the actual perceptions or behaviour, but rather what was disclosed in the integrated reports. The findings are therefore dependent on the completeness of the disclosure.

4. RESEARCH FINDINGS AND INTERPRETATIONS

4.1 Disclosure of IT risks and threats

The objective of the analysis was to determine if the companies disclosed the IT risks and threats affecting them and, if so, which type of risks and threats were they being exposed to.

Findings

Table 1: Disclosure of IT risks and threats

	Total	Percentage	
Question 1		**Yes**	**No**
1.1 Disclosure of key IT related risks	40	57.5% (n=23)	42.5% (n=17)
If yes, has the company been exposed to any of these IT risks?			
1.1.1 Social networking	23	4.3% (n=1)	95.7% (n=22)
1.1.2 Mobile devices	23	13% (n=3)	87% (n=20)
1.1.3 Malware	23	34.8% (n=8)	65.2% (n=15)
1.1.4 Corporate espionage	23	4.3% (n=1)	95.7% (n=22)
1.1.5 IT governance	23	30.4% (n=7)	69.6% (n=16)
1.1.6 Electronic records management	23	52.2% (n=12)	47.8% (n=11)
1.1.7 Data management	23	43.5% (n=10)	56.5% (n=13)
1.1.8 Cloud computing	23	0% (n=0)	100% (n=23)
1.2 Disclosure of IT related threats	40	47.5% (n=19)	52.5% (n=21)
If yes, has the company been exposed to the following categories of IT threats:	19	100% (n=19)	0% (n=0)
1.2.1 Data driven threats. If yes, to which specific data driven threats has the company been exposed to?	19	89.5% (n=17)	10.5% (n=22)

Viruses	19	57.9% (n=11)	42.1% (n=8)
Worms	19	57.9% (n=11)	42.1% (n=8)
Data corruption	19	73.7% (n=14)	26.3% (n=5)
Disk failure	19	47.4% (n=9)	52.6% (n=10)
Network problems	19	47.4% (n=9)	52.6% (n=10)
1.2.2 Business driven threats. If yes, to which specific business driven threat has the company been exposed to?	19	84.2% (n=16)	15.8% (n=3)
System availability failures	19	84.2% (n=16)	15.8% (n=3)
Application outage	19	26.3% (n=5)	73.7% (n=14)
Workplace inaccessibility	19	15.8% (n=3)	84.2% (n=16)
1.2.3 Event driven threats. If yes, to which specific event driven threat has the company been exposed to?	19	52.6% (n=10)	47.4% (n=9)
Failure to meet industry standards	19	10.5% (n=2)	89.5% (n=17)
Political events	19	0% (n=0)	100% (n=19)
Natural disasters	19	15.8% (n=3)	84.2% (n=16)
Power failures	19	26.3% (n=5)	73.7% (n=14)

Source: Control sheet used for content analysis (own calculation)

From the literature reviewed, it is evident that IT risks need to be identified by organisations to ensure that they are included in risk management processes. The findings indicate that only 57.5% of the companies disclose IT risks as key risks that they were exposed to. The findings indicate that electronic records management was the biggest IT risk faced by the companies with 52.2% of the companies listing this risk. The 13% and 4.3% of the companies were not exposed to risks concerning mobile devices, corporate espionage and social networking.

The findings indicate that IT risks can be divided into three categories and that organisations should take notice of these types of threats. The findings further reveal that 47.5% of the companies disclosed the IT threats to which they were exposed; 89.9% of the companies were exposed to data-driven threats; 84.2% were exposed to business-driven threats and 52.6% were exposed to event-driven threats.

Data corruption was the highest data-driven threat (73.7%), system availability failure was the highest business-driven threat (84.2%) and power failure (26.3%) was the highest event-driven threat.

4.2 IT steering committee, CIO and the importance of IT governance

The objective of this analysis was to identify if the company has a separate IT steering committee and a CIO and to further explore if IT governance was a regular item on the agenda of the board.

Findings

Table 2: IT steering committee, CIO and the importance of IT governance

	Total	Percentage	
Question 2		**Yes**	**No**
Does the company have a separate IT steering committee?	40	37.5% (n=15)	62.5% (n=25)
Does the company have a Chief Information Officer?	40	32.5% (n=13)	67.5% (n=27)
Is IT governance an important priority for the Board of Directors? Is it a regular item on the agenda?	40	97.5% (n=39)	2.5% (n=1)

Source: Control sheet used for content analysis (own calculation)

An IT steering committee should be established as per the King III Code on Corporate Governance. The findings show that only 37.5% of the companies implemented a separate IT steering committee. IT may form part of the duties of the audit or risk committees for the remaining 62.5% of companies, as the majority neither deem it necessary to have a separate IT steering committee nor do they feel that it can form part of another committee. The analysis also indicated that the implementation of an IT steering committee was industry- or sector-driven. If the company operated in an IT-driven industry, an IT steering committee would be appointed. The results indicated that 15 out of the 40 companies operated in an IT-driven industry.

The CEO of a company should appoint a CIO to oversee the IT steering committee and IT governance. However, the findings indicated that only 32.5% of the companies

appointed a CIO, while 67.5% did not. Once again, the appointment of a CIO was industry or sector driven. If a company operated in an IT-driven industry, a CIO was appointed. The results indicated that 13 out of the 15 companies operating in an IT-driven industry appointed a CIO.

The findings indicated that 97.5% of the companies included IT as a regular item on the board's agenda while only 2.5% of the companies indicated that IT governance was not yet successfully applied.

4.3 Risk Committee and CRO

The objective of this analysis was to explore if the company had a risk committee, if so, who formed part of this committee and if the company have a CRO.

Findings

Table 3: Risk Committee and Chief Risk Officer

	Total	Percentage	
Question 3		**Yes**	**No**
Does the company have a Risk Committee?	40	90% (n=36)	10% (n=4)
3.1 If yes, does the Risk Committee comprise the following individuals:	36	100% (n=36)	0% (n=0)
Executive members	36	41.7% (n=15)	58.3% (n=21)
Non-executive members	36	94.4% (n=34)	5.6% (n=2)
Members of senior management	36	5.6% (n=2)	94.4% (n=34)
Independent risk management experts	36	11.1% (n=4)	88.9% (n=32)
Does the company have a Chief Risk Officer?	40	42.5% (n=17)	57.5% (n=23)

Source: Control sheet used for content analysis (own calculation)

The governance of risk is an important principle included in the King III Code on Corporate Governance, which recommends that organisations establish a risk committee. The findings highlighted that 90% of the companies established a separate risk committee, while 10% of the companies did not have a separate risk committee but combined their audit and risk committees. The findings also indicated that 94.4%

of risk committee members included independent non-executives while 41.7% of the members were executives. The findings revealed that only 11.1% of the risk committees included independent risk experts and 5.6% included members of senior management. It can be concluded that the majority of the companies are aware of the importance of a risk committee.

The CEO is to appoint a CRO responsible for the governance of risk and the management of the risk committee. The findings showed that only 42.5% of the companies appointed a CRO, while 57.5% of the companies had not appointed a CRO.

4.4 Governance of risk

The objective of this analysis was to determine if the BOD ensured that there were annual risk assessments, if there was an appropriate risk response and continuous risk monitoring by management, if the BOD received assurance regarding risk management and risk disclosure, what data was received for the risk management process, and if there was an effective risk management process.

Findings

Table 4: Governance of risk

	Total	Percentage	
Question 4		**Yes**	**No**
Does the Board of Directors ensure that there are annual risk assessments?	40	100%	0%
Does the Board of Directors ensure that there are appropriate risk responses?	40	100%	0%
Does the Board of Directors ensure continual risk monitoring by management?	40	100%	0%
Does the Board of Directors receive assurance regarding the effectiveness of the risk management process?	40	100%	0%
Are there processes in place for complete, relevant, accurate, timely and accessible risk disclosure to stakeholders?	40	100%	0%
Does the company have procedures in place to ensure that they receive good, accurate and timely data regarding risks for the risk management process?	40	100%	0%
Does the company make use of an effective risk management process?	40	100%	0%

Source: Control sheet used for content analysis (own calculation)

In terms of the governance of risk, it is recommended by King III that the BOD ensure that there are annual risk assessments, risks responses and continual risk monitoring by management. The BOD should receive assurance regarding risk management and the company should have procedures in place to ensure risk disclosure to stakeholders. The company needs procedures in place to ensure that the BOD receives good, accurate and timely data regarding the risks and that an effective risk management process is implemented.

The findings showed that 100% of the companies implemented the principle of the governance of risk.

4.5 IT risk management framework

The objective of this analysis was to identify if the company made use of a specific IT risk management framework to help identify IT risks.

Findings

Table 5: IT risk management framework

	Total	Percentage	
Question 5		**Yes**	**No**
Does the company make use of a specific IT risk management framework?	40	30% (n=12)	70% (n=28)

Source: Control sheet used for content analysis (own calculation)

Organisations which identified IT risks as one of their key risks should consider implementing an IT risk management framework. The findings indicated that only 30% of the companies implemented an IT risk management framework, which is a concern given the profound impact IT risk can have on an organisation.

4.6 Governance, risk and compliance

The objective of this analysis was to determine if the BOD viewed governance, risk and compliance as one combined process or three different processes and to identify if use is made of an automated governance, risk and compliance process.

Findings

Table 6: Governance, risk and compliance

	Total	Percentage	
Question 6		**Yes**	**No**
Does the Board of Directors see governance, risk and compliance as one process?	40	100%	0%
If yes, does the company make use of an automated governance, risk and compliance process?	40	100%	0%

Source: Control sheet used for content analysis (own calculation)

Governance, risk and compliance should be seen as one process and an automated governance, risk and compliance process should preferably be used. The findings indicated that 100% of the companies see governance, risk and compliance as one process and have implemented an automated governance, risk and compliance process.

4.7 Enterprise risk management process

The objective of this analysis was to explore if the company made use of enterprise risk management and if so, whether the ERM process and the IT function worked together to identify IT risks. This analysis also sought to identify whether the risk committee included IT executives.

Findings

Table 7: Enterprise risk management

	Total	Percentage	
Question 7		**Yes**	**No**
Does the company make use of enterprise risk management?	40	47.5% (n=19)	52.5% (n=21)
If yes, does the risk management and the IT function work together?	19	94.7% (n=18)	5.3% (n=1)
If yes, does the risk committee include IT executives?	19	94.7% (n=18)	5.3% (n=1)

Source: Control sheet used for content analysis (own calculation)

A key element that needs to be present for an effective ERM is timely information; incorporating IT can assist in this regard. It was also indicated that organisations which implement an ERM system could ensure that their IT function and risk function work together. The findings indicated that 47.5% of the companies used ERM.

5. RECOMMENDATIONS AND AREAS FOR FUTURE RESEARCH

The study focused on the role of IT in the risk management processes of businesses in South Africa, specifically the top 40 companies listed on the JSE. Subsequent to the release of the King IV Report on Corporate Governance in South Africa and further recommended principles on IT risks, it is suggested that a similar study be conducted focusing on the King IV Report for Corporate Governance in South Africa.

6. CONCLUSION

The study explored the role of IT within the risk management processes of organisations, with a specific focus on good IT and risk governance. It was found that IT was an important component that should be incorporated into the risk management processes of organisations to ensure that they manage their IT risks effectively. The literature also revealed that IT played very specific roles when it came to risk management processes. The biggest role was ensuring that the risk management process receives timely and accurate information.

The empirical study found that while organisations were effective at mitigating IT risks and threats, there was room for improvement when it came to the implementation of specific IT risk management frameworks. The results also revealed that organisations understood the importance of IT when it came to the governance, risk and compliance processes, however, few organisations used ERM programmes.

To ensure that organisations are able to handle the rapidly changing IT environment, it is important to incorporate IT into risk management processes. It is also of the utmost importance to ensure that organisations understand the pivotal role played by IT in the risk management process.

Reference List

Abdolghassem, R., Mehdi, G., Hessam, P., Alireza, S., Amirhesam, H. & Simin Seifi, Z. (2013). A review of risk management and its relationship with information systems. *Arabian Journal of Business Management Review*, 2, 1–7.

Adams, S., Ruiz, C. & Rivera, E. (2013). *Governance, risk and compliance*. Monterrey: ISACA.

Anand, S. (2010). Technology and the integration of governance, risk management and compliance. *The Financial Executive,* 26(10), 57–58.

Committee of Sponsoring Organisations (COSO) of The Treadway Commission. (2004). *Enterprise Risk Management – Integrated Framework*. Available from: http://www.coso.org/documents/coso_erm_executivesummary.pdf (Accessed on 12 September 2016).

De Haes, S. & Van Grembergen, W. (2008). Practices in IT governance and business/IT alignment. *Information Systems Control Journal*, 2, 1.

Ernst & Young. (2013). *Managing risks in a fast-changing environment*. Available from: http://www.ey.com/Publication/vwLUAssets/Managing_IT_risk_in_a_fast_canging_environment/$FILE/IT_Risk_Management_Survey.pdf (Accessed on 21 July 2016).

Federation of European Risk Management Associations (FERMA). (2002). *A Risk Management Standard*. Available from: https://www.theirm.org/media/886059/ARMS_2002_IRM.pdf. (Accessed on 21 July 2016)

FNR Solutions Inc. (2016). *The importance of information technology in today's world.* Available from: https://www.linkedin.com/pulse/importance-information-technology-todays-world-fnrsolutions-inc (Accessed on 3 April 2017).

Hopkin, P. (2017). *The fundamentals of risk management.* 4th edition. Kogan Page Limited. Available from: http://www.hostgator.co.in/files/writeable/uploads/hostgator12628/file/fundamentalsofriskmanagement.pdf (Accessed on 21 July 2016)

IBM Global Technology Services. (2011). *Supporting information technology risk management*. Available from: https://www-935.ibm.com/services/multimedia/Supporting_Info_Technology_Risk_Mgmnt.pdf (Accessed on 21 July 2016).

Information Systems Audit and Control Association (ISACA). (2015). *Risk IT framework for management of IT related business risks*. Available from: : http://www.isaca.org/knowledge-center/risk-it-it-risk-management/pages/default.aspx (Accessed on 21 July 2016).

Institute of Directors. (2009). *The King Code (King III) for South Africa*. Available from: https://cdn.ymaws.com/www.iodsa.co.za/resource/resmgr/king_iii/King_Report_on_Governance_fo.pdf (Accessed on 21 July 2016)

Investor's Business Daily. (2014). *Business Risks Rise Worldwide Companies.* 1, April.

IT Business Edge. (2016). *The role of technology in GRC*. Available from: http://www.itbusinessedge.com/slideshows/the-role-of-technology-in-grc-03.html (Accessed on 21 July 2016).

IT Governance Institute. (2007). Cobit 4.1. Available from: https://www.bauer.uh.edu/parks/cobit_4.1.pdf (Accessed on 13 July 2017)

Lainhart, J.W. (2000). Why IT governance is a top management issue. *The Journal of Corporate Accounting and Finance*, 11(5), 33–40.

Madslien, J. (2017). Digitise or die. *Professional Engineering*, 30(7), 46–51.

Marx, B. (2008). *An analysis of the development, status and functioning of audit committees at large listed companies in South Africa.* Doctoral thesis. Johannesburg: University of Johannesburg.

Mizoguchi, T. (2012). *Information Technology risks in today's environment*. Available from: https://www.theiia.org/chapters/pubdocs/52/SD_IIA___ISACA_Event_041112_Deloitte_IA_Top_Ten_Risks.pdf (Accessed on 21 July 2016).

Mohamad, A.A., Ramayah, T. & Lo, M. (2017). Knowledge management in MSC Malaysia: The role of Information Technology capability. *International Journal of Business & Society,* 18, 651–660.

National Institute of Standards and Technology (NIST). (2015). *IT Risks.* Available from: http://www.opensecurityarchitecture.org/cms/definitions/it-risk (Accessed on 2 August 2016).

Optimal Networks (2017). *How (and how much) are organisations spending on IT?* Available from: http://www.optimalnetworks.com/how-and-how-much-it-spending/ (Accessed on 13 July 2017).

Patterson, T. (2015) *The use of information technology in risk management*. Financial Reporting Centre. https://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/DownloadableDocuments/ASEC_Whitepapers/Risk_Technology.pdf (Accessed on 21 July 2016)

PricewaterhouseCoopers (PWC). (2017). IT Governance, Risk and Compliance. Available from: http://www.pwc.com/la/en/risk-assurance/it-grc.html (Accessed on 13 July 2017).

Tohidi, H. (2011). The role of risk management in IT systems of organisations. *Procedia Computer Science*, 3, 881–887.

Wessels, P L. (2006). The South African business environment in which accountants function and the role of information technology in that environment. Meditari Accountancy Research, 14(2): 131–149.

Wessels, P.L. & Steenkamp, L.P. (2007). The ability of students to convert their knowledge of IT concepts into IT competencies. *Meditari Accounting Research*, 15(2),113–129.

Wilkinson, M. (2011). The role of information technology in risk management. Available from file:///C:/Users/belindas/Downloads/TW-EU-2011-20552%20(5).pdf (Accessed on 13 July 2017).

Woodard, J. (2013). *Managing IT risks and compliance: A major growing concern*. Available from: http://blog.aicpa.org/2013/07/managing-it-risks-and-compliance-a-growing-major-concern.html#sthash.pDVfvDjo.dpbs (Accessed on 21 July 2016).