IT RISK MANAGEMENT DISCLOSURE IN THE INTEGRATED REPORTS OF THE TOP 40 LISTED COMPANIES ON THE JSE LIMITED

Ben Marx*, Covanni Hohls-du Preez*

* University of Johannesburg, South Africa

OPEN ACCESS

How to cite this paper:
Marx, B., & Preez, C.H. (2017). IT risk management disclosure in the integrated reports of the top 40 listed companies on the JSE limited. *Risk governance & control: financial markets & institutions, 7(3),* 27-34. doi:10.22495/rgcv7i3p3

How to access this paper online:
http://dx.doi.org/10.22495/rgcv7i3p3

ISSN Online: 2077-4303
ISSN Print: 2077-429X

Received: 18.02.2017
Accepted: 18.05.2017

JEL Classification: M1, M15
DOI: 10.22495/rgcv7i3p3

Abstract

Information Technology (IT) has become an integral part of virtually all modern day organisations. The advent of IT has given rise to numerous benefits which increase productivity and efficiency in the workplace, however, IT also brings with it significant risks that can have an impact on an organisation's ability to function as a going concern. Organisations, especially those listed on the Johannesburg Stock Exchange (JSE), are required to submit an Integrated Report (IR) on an annual basis in which they indicate how they used the resources at their disposal to create value for the organisation and its stakeholders during the year under review. The IR is also a forward-looking document, as opposed to the traditional, backward-looking reports. The purpose of this paper is to determine to what extent IT Risk and IT Risk Management are disclosed in the IR's of the Top 40 Listed Companies on the JSE. It further aims to determine whether IT Risks are included as material risk in the entity's risk statements of the Integrated Report, and whether proper explanations are provided on how the materiality of the risks are determined and dealt with. This is done by means of an empirical study consisting of a content analysis of the IRs of the Top 40 listed companies on the JSE. The results of the analysis indicates that more than half of the companies included IT risk as part of their material risks and outlined appropriate and detailed processes that were followed by the company to manage those IT risks. The findings of the study accordingly support the need for communicating significant risks and the management thereof to stakeholders as part of the integrated nature of governance of entities. However, it is disconcerting that some companies are not doing this, and accordingly are not realising the need for communicating significant matters to their stakeholders and the value that informative and credible reporting will bring to an entity's Integrated Report.

Keywords: Risk Management, IT Risk Management, Integrated Reporting, International Integrated Report Committee (IIRC) Framework

1. INTRODUCTION

Information Technology (hereafter IT) has become an integral part of modern day business. From the early beginnings of IT in the 1960s, where working on a computer was a specialised task in terms of data processing, to the development of the personal computer in the mid-1990s, much advancement have been made in the field of IT (Gartenberg, 2006:18). The rapid development of IT in recent years has made it easier for the stakeholders of an organisation to interact with each other while carrying out their business functions. IT even allows cross-function collaborations when it comes to product development, marketing and customer services (Tseng, 2008:150).

The biggest development in IT over recent years has been the internet, which in a certain sense, has caused international boundaries between companies to disappear and has created a more 'instant' world. Gartenberg (2006:18) supports this by stating that "we live in a world of multiple devices networked locally and globally and often owned and operated by the end user. Information is shared on and distributed in real time". Sanders (2007:1334) further supports the impact of the internet on the way business is conducted by saying that "of all the IT, the emergence of the internet may

have had the greatest impact on information exchange between buyers and sellers".

In order to remain competitive in the modern economy, it is important to ensure prices stay on par with those of competitors and that products are readily available and of good quality. IT, when implemented correctly, can assist in keeping production costs as low as possible and can differentiate the organisation from its competitors (Rivard, Raymond & Verreault, and 2006:30). Effective IT systems which are managed correctly ensure constant communication between the organisation and its supplier. The result of this direct communication is the quick and reliable delivery of products when and where they are needed (Sanders, 2007:1334).

From the discussion above, it is clear that the development of IT over the years has brought a significant amount of benefits to modern day businesses, but with these advances, there came additional risks as well.

The purpose of this paper is to determine to what extent IT Risk and IT Risk Management is disclosed in the IR's of the Top 40 Listed Companies on the JSE and whether it is in the format as required by the IR Framework. It further aims to determine whether IT Risks are included as material risk in the entity's risk statements of the Integrated Report, and whether proper explanations are provided on how the materiality of the risks are determined and dealt with.

The remainder of this paper is set out as follows. The following section presents the objectives, scope and limitations of the study. The sections thereafter describe the theoretical background of the paper, the methodology applied and the empirical findings and deductions. Recommendations drawn from the study are then provided, and conclusions are presented in the last section.

2. OBJECTIVES, SCOPE AND LIMITATIONS

The objective of this paper is to determine the extent to which IT Risk and IT Risk Management are disclosed in the Integrated Reports (IRs) of organisations. The methodology followed to achieve this objective consists of a literature review, based on which a critical analysis is conducted to identify IT risks that organisations are exposed to as well as the way in which these risks are being managed. The literature review also provides guidance on how an IR should look, what should be considered when preparing an IR and what should be included. The results of the literature review form the basis for a content analysis of the IRs of the Top 40 listed companies on the Johannesburg Stock Exchange (JSE).

There are limitations to this study as the empirical study is limited to the Top 40 listed companies of the JSE only, and may not be representative of the smaller, listed entities on the JSE. However, the reason for selecting the Top 40 JSE companies as a population is due to the fact that they represent 83.31% market share of the total market as at 7 September 2016 (JSE, 2016(b)). An expectation is created that if the Top 40 listed companies on the JSE are providing quality IRs, smaller companies will have be provided with a good example to work from when producing their own IRs. All Top 40 listed companies were included in the empirical study.

3. LITERATURE REVIEW

3.1. Information Technology risks

With IT forming such an integral part of modern day business, companies face many new risks. This is emphasised by Marx (2008:82) who is of the opinion that "the development of IT, electronic commerce and increased reliance and dependency on IT resources have exposed modern businesses to many challenges and significant new risks". IT Risks can be defined as "any event or action that could cause a loss or damage to computer hardware, software, data or information" (Wong, 2016). IT Risks can be divided into five main groups. Each of these groups has its own smaller elements and these elements can sometimes be found in more than one group (Parent & Reich, 2009:142). The five groups identified are:

- IT Competence risk which refers to the IT knowledge of the directors of an organisation;
- IT Infrastructure risk which refers to the risk of computers, networks, operating systems, applications and databases of an organisation not functioning as intended;
- IT Project risk which refers to the risk typical of a new and large project being undertaken which is related to IT specifically;
- IT Business Continuity risk which refers to the risk of the organisation not being able to function in the event of a disaster due to the loss of critical information; and
- IT Information / Security risk which refers to the risk of unauthorised persons gaining access to confidential and sensitive information.

It is important for an organisation to inform current stakeholders and potential investors of the additional risks that companies face due to the presence of IT and how those risks can affect the organisation.

3.2. Risk disclosure in the Integrated Report

According to International Accounting Standard 1 (IAS 1) as set by the International Accounting Standards Board (IASB), companies are required to provide annual general purpose financial statements. IAS 1 defines general purpose financial statements as "those intended to meet the needs of users who are not in a position to require an entity to prepare reports tailored to their particular information needs" (IASB, 2011). According to Amran, Che Haat and Manaf Rosli Bin (2008:39), the annual report of an organisation, which consists of financial and non-financial information, has been the chief means of conveying useful information for investment, credit and other decisions over the years. In modern day reporting, individual statements such as the Statement of Comprehensive Income and the Statement of Financial Position are not released on their own anymore; the IR has replaced the individual statements with one report, to be issued to all stakeholders, which is aimed at providing stakeholders with a comprehensive view of the organisation. The IR tends to present a more holistic picture of the organisation's strategy instead

of just providing purely financial information. Most organisations have used their annual reports as a basis and have included the elements of an IR, renaming their reports as Annual Integrated Reports. However, through this method of reporting, the page number of reports has increased significantly and there may be the risk of too much information being imparted at once (de Villiers, Rinaldi & Unerman, 2014:1045).

Risk is a very important part of disclosure, but it is often not presented with enough consultation and care. One of the possible reasons for not giving adequate attention to risk disclosure is the fear of management of the possible negative effects such disclosure may have on the organisation. This notion is echoed by Deumes (2008:123) who says that "managers may perceive that there is a cost imposed on the organisation by competitors who exploit the information to the detriment of the disclosing organisation".

However, by disclosing risks, managers can increase the transparency and reliability of the IR. Disparities can also be reduced between management's ability to deliver and what an investor understands (Deumes, 2008:122). Investors will gather as much information as possible on risks before they make an investment decision (Amran et al., 2008:42). Clear, readable and understandable disclosure results in stronger reactions from investors, especially small investors. This leads to more positive reactions when there is good news and more negative reactions when there is bad news (Rennekamp, 2012:1343). Proper risk disclosure reduces potential investors' uncertainty in terms of future organisation cash flows (Gao, 2010:3). Sometimes, even customers, staff and other stakeholders benefit from risk disclosure (Miihkinen, 2012:441). Part of risk disclosure is not just to report on the risk, but as stated by Miihkinen, to provide information on how this risk is managed to increase shareholders' wealth and limit the possibility of financial failure (Miihkinen, 2012:441).

From the discussion above, it is evident that organisations ought to disclose their specific risks. The disclosure of risk helps to ensure transparency and provide insight into current investments; it assists stakeholders with decision-making and helps potential investors with investment decisions.

3.3. IT Risk Management

Risks are an important part of an organisation's business activities. This is evidenced in the fact that it is mandatory in certain industries such as the banking sector to have a Risk Management system in force (Ecker-Lala, 2010:218). Attributed to globalisation and the increased connectivity of organisations, risks are evolving at a rapid pace. Change, including IT developments, is advancing at an ever-increasing rate, requiring Risk Management to constantly adapt to what is termed the 'new normal' (Institute of Directors, 2016:18). Nocco and Stulz (2006) place further emphasis on the fact that organisations need to take note of changes in how business is conducted. They are of the opinion that the changes that have occurred over the past few years, coupled with the continuous reliance placed on IT networks, have brought about a significant shift in the Risk Management role of an organisation (Nocco & Stulz, 2006:8).

Effective Risk Management and proper Risk Management procedures to monitor risks in a consolidated manner give an organisation a competitive edge over one which assesses and monitors risks on an individual basis (Nocco et al., 2006:8). Effective Risk Management enables an organisation to take more strategic business risks and use opportunities relating to its core business for the benefit of the organisation (Nocco et al., 2006:9). One of management's essential roles in an organisation is to mitigate risk. In order to ensure the negative impact of risks on an organisation is eliminated or at least kept to a minimum, possible risks that can be encountered during the course of business have to be identified at an early stage and managed with the correct level of skill (Ahmed, Capretz, Sandhu & Raza, and 2014:280).

Jalba and Anicai (2012:0531) define IT risk as a sub-set of business risk, which is a consequence of business decisions. Over the past few decades, IT applications have become more susceptible to risk. This is due to the widespread use of computers, the rapid development of the internet and the interconnectivity of computers. Another reason for the increased risk is users' improved IT skills. This increase in risk requires that greater attention be given to the management of IT Risk (Farah, 2011:13). IT Risk Management is a sub-set of the overall Risk Management responsibilities of the board of directors (Parent & Reich, 2009:137). The approach for IT Risk Management is, in general, the same as for Risk Management. The only difference between general Risk Management and IT Risk Management is the fact that IT Risk Management focuses first on IT risks which are then incorporated into the general Risk Management of an organisation. The need to manage IT Risks has led to the development of several risk assessment frameworks by professional bodies (Al-Ahmad & Mohammad, 2013:29). The need for such frameworks can be attributed to the fact that research has shown that many boards pay insufficient attention to IT Risk Management. Studies have shown that the most common reason for this is the fact that the IT Strategy does not align with business strategies. Parent and Reich (2009:137) further indicate a significant lack of interest in IT by boards of directors.

One of the best risk assessment frameworks for IT is the COBIT 4.1 (Control Objectives for Information and Related Technology). COBIT 4.1 was developed by the Information Systems Audit and Control Association (ISACA) and adopts a more holistic approach to Risk Management than other standards. It focuses on identifying control objectives and developing controls to meet the identified objectives. It consists of 34 processes that manage and control information and supporting technology. Research conducted on organisations over the years has shown that COBIT has assisted in the alignment of business and IT to create an IT Governance Framework and establish IT Risk Management in organisations (Al-Ahmad et al., 2013:33).

IT Governance can be defined as "the decision rights and accountability framework to encourage desirable behavior in using IT" (Juiz, Guerrero & Lera, 2014:14).The King IV report on Corporate Governance recognises the importance of IT in

modern day organisations and the risks associated with it. A separate section has therefore been devoted specifically to governing IT risks. Thus, Principle 4.2 in King IV states that the "governing body should govern technology and information in a way that supports the organisation in defining its core purpose and achieving strategic objectives" (Institute of Directors, 2016:53).

King IV also provides guidance on IT Risk Management issues that should be disclosed. These issues include:

- Structures and processes of IT Management;
- Key focus areas during the reporting period;
- Mechanisms in place for monitoring and assessing the adequacy and effectiveness of IT; &
- How past performance, current operations and future strategic objectives of the organisation are affected by digital development.

3.4. Purpose of integrated reporting

King IV, currently in draft format, requires an IR to 'tell the story' of how an organisation can create value in the future. This can be achieved by managing current risks that can have an impact on value creation in the future, especially if they are material risks. It requires an IR to adopt a forward-looking approach into the future and determine whether the organisation can deliver in terms of value (IoD, 2016:12). The importance attached by King IV to the release of an IR is such, that one of the principles of the report states that "the governing body should ensure that reports and other disclosures enable stakeholders to make an informed assessment of the performance of the organisation and its ability to create value in a sustainable manner" (IoD, 2016:37). One of the practices recommended by King IV stipulates that an organisation should issue an annual report in which all material information is presented in an integrated manner and provides a stakeholder with a clear, holistic, concise and understandable representation of the performance of the organisation. King IV requires some of the minimum requirements to be present in an IR as per the IIRC's IR Framework in its recommended practices (IoD, 2016:37).

Internationally, the first real attempt to formalise IRs occurred in 2010 when the International Integrated Reporting Committee, later the International Integrated Reporting Council (IIRC), was founded by two of the leading organisations in the field of accounting for sustainability, namely, The Prince's Accounting for Sustainability Project (A4S) and the Global Reporting Initiative (GRI) (Flower, 2015:1). The origins of these bodies can be traced back to a speech made by the Prince of Wales in 2009 when he called for the existence of such a body (Flower, 2015:1). The primary purpose of the IIRC was to provide a concise (relatively few pages) report to indicate an organisation's most material social, environmental and economic actions, outcomes, risks (including IT Risks) and opportunities in such a manner that reflects the integrated nature of these factors for the organisation (de Villiers et al., 2014:1046). In order to provide a concise account indicating value creation over time, an organisation needs to communicate its strategy, governance, performance and prospects in the context of its external environment to show short-, medium- and long-term value creation (Cheng et al., 2014:92).

4. METHODOLOGY

The methodology followed in the study consists of a literature review, based on which a critical analysis was conducted to identify IT risks that organisations are exposed to and determine how these are being managed. The review also provides guidance on how an IR should look, what should be considered when preparing an IR and what should be included. The results of the literature review thus form the basis of a content analysis of the IRs of the Top 40 listed companies on the Johannesburg Stock Exchange (JSE).

4.1. Population

The population selected for testing consists of the Top 40 listed companies on the JSE. The JSE Top 40 companies are reviewed on a quarterly basis in March, June, September and December of every year as part of the FTSE / JSE quarterly index review (2016(a):22). The population for the empirical study was selected based on the Index as at 7 September 2016 (JSE, 2016(b)). The reason for selecting the Top 40 companies of the JSE as a population is due to the fact that they represent 83.31% market share of the total market as at 7 September 2016 (JSE, 2016(b)).

4.2. Content Analysis

The empirical study consists of a content analysis of the IRs or Annual IRs of the Top 40 listed companies on the JSE. Content analysis is widely recognised and supported as a suitable research instrument for understanding and analysing the characteristics of a selected population (Marx & Mohammadali-Haji, 2014:235). This is confirmed by Ceci and Iubatti who agree that content analysis can be used to analyse a given set of data to ensure the objective, systematic and quantitative description of the communication contents of the data set (Ceci & Iubatti, 2012:566).

5. RESEARCH FINDINGS AND INTERPRETATION

5.1. Type of reporting

Objective of the analysis

The purpose of this section is to determine how many of the Top 40 listed companies on the JSE produce an IR and in what format.

Findings and deductions

Table 1. Type of reporting

Type	*Number*	*%*
Integrated Annual Report (annual report and financial statements combined)	26	65
Separate Annual Report and Integrated Report	12	30
Annual Report only (no Integrated Report)	2	5
Total	**40**	**100**

Source: Own analysis

The above findings indicate that most of the companies provide annual IRs consisting of Annual

Financial Statements and IR information, as required by the IR Framework. The layout of these reports takes the form of an annual report where the elements of an IR have been included to create one, complex report. The annual IR, where the elements of the IR have been included in the annual reports, clearly indicates the relevant information as required by the IR framework, and the financial statement section of the report is clearly indicated. However, some companies merely renamed their annual reports as Integrated Annual Reports in order to give the impression that an IR was provided, when in fact that was not the case.

It became evident that the format of the reports, irrespective of whether they were annual reports or integrated annual reports, was fairly similar. Both of these types of reports generally contain the following sections: strategic overview of the organisation, business review, governance report, key risks and opportunities or risk management report or material risk, financial overview or financial statements.

The companies which produced standalone IRs provided a relatively concise document which included the information required by the IR framework. Risks were clearly indicated and there was sufficient reference made to other reports available on the organisation's website where more details could be obtained.

5.2. Disclosure of how material risks are determined

Objective of the analysis

The objective of this part of the analysis was to determine which of the 38 companies that produced IRs or Annual Integrated Reports provided stakeholders with an explanation as to how the material issues / risks were identified.

Findings and deductions

Table 2. Disclosure of whether discussion is provided on how material risks have been identified

Element	*Numbers*		*Percentages*		*Total*
	Yes	*No*	*Yes*	*No*	
Discussion provided on how material risks have been identified	23	15	61%	39%	**38**

Source: Own analysis

The analysis indicated that only 23 of the companies provided information to stakeholders on how material risks were being identified. The companies that did not provide explanations on how material risks were determined simply provided the disclosure of their material risks.

Some of the main processes followed by the companies to identify material risks include, but are not limited to:

- Determining the likelihood and potential impact of the risk on the organisation;
- Identifying the risks that could lead to a breach of the organisation's risk appetite and impact the value chain negatively;
- Issues that could have an impact on achieving the commercial viability and social vision in the medium term;
- Risks that could have a material impact on the reputation of the organisation;
- Key matters that could have an impact on the organisation achieving its strategic objectives and creating value; and
- Matters that could affect the business model, future performance, solvency or liquidity of the organisation.

5.3. Disclosure of material risks

Objective of the analysis

The objective of this part of the analysis was to determine how many of the 38 companies which provided an IR or Annual Integrated Report disclosed material risks that could have an impact on value creation over the short, medium and long term. Furthermore, this part also sought to determine how many of the companies which did disclose material risks included IT risk as a material risk. Where IT risks have been included as a material risk, the analysis went further to determine whether the IT risk was easily identifiable or not.

Findings and deductions

Table 3. Disclosure of material risk

Element	*Numbers*		*Percentages*		Total
	Yes	*No*	*Yes*	*No*	
Material risk is properly disclosed	35	3	92%	8%	**38**
IT Risk is included in Material risk	23	12	66%	34%	**35**
IT Risk is easily identifiable	20	3	87%	13%	**23**

Source: Own analysis

The findings above indicate that the majority of the organisations (92%) provided disclosure of their material risks. These risks were spread throughout the organisation and were not limited to only financial risks. It is interesting to note that IT is deemed a significant risk for only 66% of the population. Of the 23 companies which included IT risk as part of material risks, 20 disclosed the IT risks in a manner that was easily identifiable to the stakeholder. Whether IT risk was deemed a material risk depended on the industry type. Throughout the banking industry, IT was deemed to be a material risk. Most of the mining organisations did not deem IT risk as a material risk, however, they all disclosed that IT Governance was being applied appropriately. Those organisations in the mining industry which identified IT risk as a material risk did so primarily in terms of the risk of unauthorised access to their systems, confidential information and security breaches that could take place. Risks that were material to the mining industry included the economy, constant supply of electricity and climate change. The retail industry, in general, did not classify IT risk as a material risk with the exception of the Woolworths Group where IT risk was disclosed as being a material risk. Other industries where IT risk was classified as a material risk

included the beer industry, the printing industry, telecommunications, the medical industry, packaging, investment (primarily due to client information that has to be kept confidential) and the medical aid industry.

The results of the analysis further indicate that where material risks were discussed, including IT risks, the risks were easily identifiable.

5.4. The detail in which IT risk is disclosed

Objective of the analysis

This part of the analysis sought to determine the level of detail in which the IT risks were disclosed, in particular, to establish whether there was simply a high-level mention of IT risks or whether risks were discussed individually.

Findings and deductions

Table 4. Detail in which IT risks are disclosed

Element	*Numbers*		*Percentages*		Total
	Yes	*No*	*Yes*	*No*	
IT Risk disclosed with sufficient detail	20	3	87%	13%	**23**

Source: Own analysis

From Table 4 above, it is evident that 87% of the companies disclosed their IT risks with enough detail to give the stakeholder sufficient information on their IT risks. Some of the material IT risks that were identified and disclosed during the analysis included, but were not limited to:

- Cyber attacks, which are growing more sophisticated on a daily basis and can have an adverse impact on the marketing of an organisation, as well as increased money laundering and financial fraud;
- Disruption to IT systems which could lead to the loss of valuable information;
- Unauthorised access, through breaches of the IT system, to confidential information and possible contraventions of the POPI Act;
- IT malfunction that could lead to loss of data and key information;
- The loss of competitive advantage due to the fast-changing IT environment;
- The inability of infrastructure to keep up with changes in the IT environment;
- Inadequate systems / investments in IT;
- IT systems not being fully aligned to support business processes and procedures; and
- Disruption in business operations and business continuity.

Risks differ from organisation to organisation, but the one threat that is consistent in each organisation is the risk that access may be obtained by unauthorised persons to sensitive information.

5.5. Extent of detail in which IT Risk Management is disclosed

Objective of analysis

The purpose of this part of the analysis was to determine how many of the companies that disclosed IT risk with sufficient detail, disclosed the procedures followed to manage this risk with an equal amount of detail.

Findings and deductions

Table 5. Detailed IT Risk Management disclosure

Element	*Numbers*		*Percentages*		*Total*
	Yes	*No*	*Yes*	*No*	
Detail with which IT Risk Management is disclosed	20	3	87%	13%	**23**

Source: Own analysis

Based on the analysis, it was evident that all organisations provided a general Risk Management process that was followed to manage risks. Organisations which disclosed IT risk as part of their material risks provided detailed Risk Management procedures as well. This meant that the Risk Management processes were either included next to the risk in the disclosure of the material risks, or they were provided in the Risk Management report included in the Integrated Annual Reports. Disclosure of IT Risk Management procedures could not be traced to specific types of Risk Management reports provided by the organisations. Where separate Risk Management reports were produced, organisations appeared to base these on disclosure in terms of IT Governance, as required by King III and King IV. Where IT risks were included in the material disclosure, detailed Risk Management processes were disclosed.

Some of the common IT Risk Management procedures followed by the companies included, but were not limited to:

- Implementing Risk Management procedures according to the framework provided by COSO;
- Constant development and implementation of IT security policies;
- Increased investment to improve IT security awareness;
- Intelligence and implementation of sound security processes;
- Building necessary resilience into systems to manage and identify cybercrime;
- Continuously assessing threats and adapting controls for risk;
- Implementing logical access controls comprehensively;
- Increasing customers' and clients' awareness of cyber threats and how to prevent these;
- Implementing and maintaining antivirus software;
- Putting into place policies and monitoring these to ensure business continuity;
- Taking out cyber insurance to assist with major cyber breaches; and
- Performing regular tests to determine the ability of the organisation to recover data within the prescribed timeframe.

6. RECOMMENDATIONS AND AREAS FOR FUTURE RESEARCH

Based on the results of the study, it is recommended that management and those responsible for the preparation of financial information obtain a thorough understanding of the purpose of an IR and the goals it should achieve with regard to stakeholders. Those charged with governance and those responsible for the preparation of financial information need to ensure that they have a thorough understanding of the IR framework as this is a useful document which provides guidance on preparing an IR. When assessing risks, it is important for modern day organisations to not just focus on financial risks or traditional risks that they currently face or may have faced over the years; careful consideration should also be given to IT risks faced by organisations and an assessment of their potential impact in the future should be made. Organisations must also include in their assessment the procedures to be implemented to manage the identified risks. It is crucial for IT risk to be included in risk assessments because IT has become the focal point of most modern day organisations.

This study focused on the disclosure of IT Risk and IT Risk Management in the IRs of the Top 40 listed companies on the JSE. It is recommended that a study similar to the present one be performed on smaller listed entities to investigate the disclosure of IT Risks and IT Risk Management as applicable to them.

Further to the above, the following areas have been identified for future research:

- An investigation into the difficulties organisations experience which can prevent them from disclosing risks in the short, medium and long term in an IR;
- The extent of competitive advantage to be gained through effective IT Risk Management procedures; and
- The impact King IV will have on entities IT Governance in terms of current IT Governance practises and disclosures in their IR.

7. CONCLUSION

This study investigates the extent to which IT Risk Management is disclosed in the IRs of the Top 40 listed companies on the JSE. The results show that most companies have included IT risk as part of material risks faced. However, although these companies did include Risk Management in their disclosures, not all of them provided sufficient evidence of detailed Risk Management procedures to be followed for each identified risk. Some provided a blanket Risk Management process discussion.

From the analysis conducted, it can be concluded that most companies disclose material risk separately and for 66% of those companies, IT risk is considered to be a material risk. Of the 66% which consider IT risk a material risk, IT risk can clearly be identified in 87% of those reports. Of the 66% companies where IT risk was included in the IR as part of material risks, 87% provided details on the specific risks faced as well as how the respective risks were managed. The empirical study thus showed that more than half of the Top 40 Listed Companies on the JSE indicated IT risk as a critical risk, especially in terms of risks relating to continuity in the event of a disaster and protection of personal / confidential information. It became clear during the course of this study that there are still improvements to be made in terms of Risk Management disclosure and the grouping of risks in the short, medium and long term when disclosure of the above is made in the IR.

To ensure greater transparency and added value for stakeholders, it is essential that the management of companies or the preparers of financial information have a thorough understanding of IRs and their purpose as well as the disclosure requirements that need to be met, especially in terms of the level of detail in which certain elements have to be disclosed.

REFERENCES

1. Al-Ahmad, W., & Mohammad, B. (2013). Addressing information security risks by adopting standards. *International Journal of Information Security Science, 2(2),* 28-43.
2. Amran, A., Manaf Rosli Bin, A. & Che Haat, M.H., (2008). Risk reporting: An exploratory study on risk management disclosure in Malaysian annual reports. *Managerial Auditing Journal, 24(1),* 39-57.
3. Ceci, F. & Iubatti, D. (2012). Personal relationships and innovation diffusion in SME networks: A content analysis approach. *Research Policy, 41(3),* 565-579.
4. Cheng, M., Green, W., Conradie, P., Konishi, N. & Romi, A. (2014). The international integrated reporting framework: Key issues and future research opportunities. *Journal of International Financial Management & Accounting, 25(1),* 90-119.
5. De Villiers, C., Rinaldi, L. & Unerman, J. (2014). Integrated reporting: Insights, gaps and an agenda for future research. *Accounting, Auditing & Accountability Journal, 27(7),* 1042-1067.
6. Deumes, R. (2008). Corporate risk reporting: A content analysis of narrative risk disclosures in prospectuses. *Journal of Business Communication, 45(2),* 120-157.
7. Ecker-Lala, W. (2010). Risk management for enterprises. *Hyperion International Journal of Econophysics & New Economy, 3(2),* 217-223.
8. Flower, J. (2015). The International Integrated Reporting Council: A story of failure. *Critical Perspectives on Accounting, 27*, 1-17.
9. Gao, P. (2010). Disclosure quality cost of capital and investor welfare. *The Accounting Review, (1),* 1-29.
10. Gartenberg, M. (2006). Technology now defines the business. *Computerworld*, *40(31),* 18-19.
11. International Accounting Standard Board (IASB) (2011). *IFRS Textbook.* London: IFRS Foundation.
12. Institute of Directors (IoD) (2016). *King Code IV on Corporate Governance in South Africa.* Retrieved September 10, 2016 from the World Wide Web: http://bit.ly/KingIVdraft.
13. Johannesburg Stock Exchange Limited (JSE) (2016a). *Ground Rules for FTSE / JSE Africa Index Series.* Retrieved September 17, 2016 from the World Wide Web: https://www.jse.co.za/contenct/JSEIndexClassificationandCodesItems/FTSE%20JSE%20Ground%20Rules.pdf.
14. Johannesburg Stock Exchange Limited (JSE) (2016b) (info@jse.co.za). 7 September 2016. *RE: Indices - Top 40 listed companies.* Email to Hols-du Preez, C. (chohls@uj.ac.za).

15. Juiz, C., Guerrero, C., & Lera, I. (2014). Implementing good governance principles for the public sector in information technology governance frameworks. *Open Journal of Accounting*, *(3)*, 9-27.
16. Marx, B. (2008). An analysis of the development, status and functioning of audit committees at large listed companies in South Africa. PhD thesis. Johannesburg: University of Johannesburg.
17. Marx, B., & Mohammadali-Haji, A. (2014). Emerging trends in accounting: An analysis of integrated reporting practices by South African top 40 listed companies. *Journal of Economic and Financial Sciences, 7(1),* 233-252.
18. Miihkinen, A. (2012). What drives quality of firm risk disclosure?: The impact of a national disclosure standard and reporting incentives under IFRS. *The International Journal of Accounting, 47(4),* 437-468.
19. Parent, M., & Reich, B.H. (2009). Governing information technology risk. *California Management Review, 51(3),* 134-152.
20. Rennekamp, K. (2012). Processing fluency and investors' reactions to disclosure readability. *Journal of Accounting Research, 50(5),* 1319-1354.
21. Rivard, S., Raymond, L., & Verreault, D. (2006). Resource-based view and competitive strategy: An integrated model of the contribution of information technology to firm performance. *The Journal of Strategic Information Systems, 15(1),* 29-50.
22. Sanders, N.R. (2007). An empirical study of the impact of e-business technologies on organizational collaboration and performance. *Journal of Operations Management, 25(6),* 1332-1347.
23. Tseng, S. (2008). The effects of information technology on knowledge management systems. *Expert Systems with Applications, 35(1),* 150-160.
24. Wong, T.S. (2016). *Computer Security Risks.* Retrieved September 25, 2016 from the World Wide Web: http://www.wong-sir.com/cit/social_impacts/computer_security_risks.htm.