INTERNATIONAL JOURNAL OF eBUSINESS AND eGOVERNMENT STUDIES
Vol 8, No 2, 2016 ISSN: 2146-0744 (Online

KING III INFORMATION TECHNOLOGY GOVERNANCE REQUIREMENTS – AN INTERNATIONAL COMPARISON

A. M. Moolman
North-West University (Vaal Campus), South Africa
E-mail: anneke.moolman@nwu.ac.za

Melinda Ngwenya
BDO, South Africa
E-mail: mngwenya@bdo.co.za

─Abstract ─

Information Technology (IT) has become essential due to its beneficial role in various aspects of business, including financial reporting. However, IT's involvement in central components of business operations have caused increasing vulnerability to companies. Thus, the risks related to IT need to be governed. Several regulations have been developed internationally to regulate IT governance. As the King Code of Governance 2009 (King III) governs IT in South African companies, the study qualitatively evaluates King III against international IT governance regulations to ensure that South African companies' IT governance compete on an international level. Findings indicate that King III leads internationally in terms of IT governance. The study contributes suggestions to further improve King III IT governance, relating to controls to prevent data tampering and data access, implementing IT risk assessment analysis processes, and policies to maintain IT security.

Key Words: *Information technology, King III, Sarbanes-Oxley Act, International Organisation for Standardisation, International Standard on Auditing 315.*

JEL Classification: M42

Vol 8, No 2, 2016 ISSN: 2146-0744 (Online

1. INTRODUCTION

Information Technology (IT) has become essential in today's economy. Its capabilities offer organisations opportunities to be innovative and to exploit all technology resources to meet organisations' objectives in a more sophisticated and strategic way (Grant, Hackney & Edgar, 2010), revolutionising nearly all aspects of business.

Although IT can enhance an organisation's efficiency and effectiveness (Markus, Bui, Jacobson, Lisein & Mentzer, 2014), it can also weaken the company's performance due to risks affecting the processing methods used in an IT environment (Loebbecke, Loebbecke & Arens, 2000). Often, IT-related risks are ignored compared to other business risks and as a result, these risks lead to substantial losses (ISACA, 2009). IT has therefore triggered a need for evolving forms of organisational governance, especially with regards to effective IT governance (Tiwana, Konsynski & Venkatraman, 2013).

1.1 Background

IT governance forms a fundamental part of corporate governance (Van Grembergen, 2013) and information thereof is important to stakeholders (Marx, 2009). IT governance regulations were therefore developed internationally, including the King Code of Governance for SA 2009 (King III), the Sarbanes-Oxley Act (SOX) and the International Organisation for Standardisation (ISO's).

King III provides guidance on corporate governance, including IT governance, for South African companies (IODSA, 2009), to place the country at the forefront of governance internationally (Du Plessis, 2009). It is therefore important to establish King III's international stance in terms of IT governance.

1.2 Possible contribution of study

IT is a vital component of organisations and its governance is necessitated by its associated risks. Previous studies have not compared different IT governance regulations with King III to evaluate its stance on an international playfield. This study contributes to the body of knowledge relating to IT governance as part of corporate governance by comparing King III IT governance requirements to that of international regulations, and providing suggestions to further improve King III IT governance requirements. Its findings may benefit governing bodies of companies, as well as regulatory bodies, to further improve South Africa's IT governance.

1.3 Research Question

The study primarily aims to answer the following research question:

How does King III IT governance requirements compare to international IT governance regulations?

To answer this question, the following secondary objectives are formulated:

- Determine IT governance requirements as per King III, SOX and ISO.
- Compare King III, SOX and ISO's IT governance requirements and provide suggestions to further improve King III IT governance requirements.

The study explored IT's history, its risks, and governance, provided an overview of King III, SOX and ISO IT governance requirements as well as a comparison of King III IT governance requirements against SOX and ISO.

2. LITERATURE REVIEW

2.1 The need to govern IT risks

IT has inspired the re-engineering of traditional company methods that were used, to promote more efficient operations and provide methods to redesign and improve communication skills within the entity and between the entity's stakeholders (Hall, 2011). IT and its constant evolvement, have however introduced new risks that require unique and effective risk governance strategies by companies (Hall, 2011), which the auditor has to foresee, and ensure the company manages and control throughout the organisation (Pickett, 2011).

According to ISACA (2009) an IT-related risk can be defined as the business risk that is associated with "*the use, ownership, operation, involvement, influence and adoption of IT within an entity*". It can occur with both uncertain frequency and magnitude, creating challenges in meeting strategic goals and objectives. IT-related risks include: unauthorised access to companies' master files resulting in breach of confidentiality, data loss, social networking which exposes companies to the risk of brand violation, malware resulting in loss of company information or corruption of the hardware, systematic and random errors, and failure to comply with IT governance regulations resulting in regulatory violations (Mar, Johannessen, Coates, Wegrzynowicz & Andreesen, 2012). IT events can no longer be confined without affecting overall business functions (IBM, 2011).

Vol 8, No 2, 2016 ISSN: 2146-0744 (Online

In terms of addressing the different IT-related risks associated with greater reliance on IT, and to improve the performance of IT, companies implement controls specific to the IT function (Loebbecke *et al.*, 2000 and Mizoguchi, 2012), leading to effective IT governance (Guldentops, 2001). In 2004, Kordel conducted research that indicated that one of the key factors distinguishing and separating top performing companies from standard-performing companies is the level of involvement and leadership of management in making key IT decisions and the manner in which IT is supported by the entity (Butler & Butler, 2010). An organisation needs to provide an equivalent level of commitment to IT governance as it allocates to other areas of corporate governance in order to achieve corporate success (Rao, 2003). The purpose is to direct IT endeavours to ensure that IT performance meets the objectives set out in an entity's strategy (Noraini, Bokolo, Rozi & Masrah, 2015), and that investments in IT add business value (Brisebois, Boyd & Shadid, 2009).

Several IT governance regulations were therefore drafted internationally. Examples of this are King III, SOX and ISO, which established specific IT governance requirements.

2.2 IT governance regulations

IT regulations provide the legal framework for collecting, storing, and disseminating electronic information in the global marketplace and the governance of IT (HG.org, 2012), and compliance is essential (National Computing Centre, 2005). All the regulations regarding IT, strive for the same goals, which are mainly to establish and implement controls, maintain, protect and assess compliance issues, identify and remediate vulnerabilities and deviations, and lastly, to provide reporting that can prove an organisation's compliance (ISACA, 2012).

2.2.1 King III requirements for IT governance

King III is the first King Code to include IT governance, recognising IT as a fundamental part of business (Hoekstra, Rajkaran & Laubscher, 2012). IT reporting should be included in the integrated report and should be complete, timely, relevant, accurate, and accessible and contain prospective information (Nkonki, 2011). The requirements of IT governance as per King III are as follows (IODSA, 2009; Nkonki, 2011; PwC, 2015):

- The Board of Directors should be responsible for IT governance: The IT governance framework supports effective and efficient management and

decision-making around the use of IT resources to facilitate the achievement of the company's objectives and the management of IT-related risks.

- IT should be aligned with the performance and sustainability objectives of the company: IT should be exploited in a way that most effectively supports and enables the business strategy, adds value and improves performance.
- The Board of Directors should delegate to management the responsibility of implementing an IT governance framework: Responsibility for the implementation of IT governance should be assigned to the Chief Information Officer (CIO), as appointed by the Chief Executive Officer (CEO). The CIO should report to the Board of Directors on the performance of the IT function.
- The Board of Directors should monitor and evaluate significant IT investments and expenditure: Value delivery and return on investment of IT should be monitored by the board.
- IT should form an integral part of the company's risk management: The Board of Directors should evaluate how IT can be used to aid the company in managing its risk and compliance requirements.
- The Board of Directors should ensure that information assets are managed effectively: The Board of Directors should ensure that processes have been established to ensure a formal information security management system is in place.
- A risk committee and audit committee should assist the Board of Directors in carrying out its IT responsibilities.

2.2.2 SOX requirements for IT governance

The USA introduced SOX (2002) after the Enron and WorldCom scandals to prevent similar scandals in the future and to protect stakeholders' investments. SOX was later adopted by other G8 countries (France, Germany, Italy and the UK) (Coetzee, Du Bruyn, Fourie & Plant, 2010).

Although South African companies are not legally compelled to comply with SOX, some South African organisations have formal alliances with the USA through shareholding or business contracts, which necessitates compliance with SOX (Coetzee *et al*., 2010).

SOX's Section 302 and Section 404 are of importance to examine the IT governance requirements (Correlog, 2011):

- **Section 302 –** This Section is intended to safeguard the company against faulty financial reporting and indicates that companies must safeguard their data responsibly as to ensure that financial reports are not established upon faulty data, interfered data, or data that may be materially inaccurate: The signing officers (the individuals or management with authorised signatory) are required to have disclosed to the auditor and the audit committee all major deficiencies in the policy or operation of internal controls. This could unfavourably affect the issuer's ability to record, process, summarise, and report financial data. The signing officers should also indicate in the report whether or not there were noteworthy changes in internal controls or other factors that could significantly affect internal controls following the date of its evaluation, including any corrective measures with regard to significant deficiencies and material weaknesses.
- **Section 404 –** This Section highlights that the safeguards mentioned in Section 302 should be disclosed and be reviewed by external auditing: The annual reports should include an internal control report. The report shall state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting. It should contain an assessment of the effectiveness of the internal control structure and procedures of the issuer for financial reporting, from the end of the most recent fiscal year of the issuer.

Although the topic of IT governance is not discussed specifically within SOX, effective and reliable internal control, including IT governance, forms the basis for compliance and prudent business practices (Correlog, 2011).

2.2.3 ISO requirements for IT governance

The norms established by ISO have a major impact on national and local environmental and social issues. It is therefore essential to consider ISO, even though it is used by companies on a voluntary basis (Morikawa & Morrison, 2004). ISO deals with IT governance and helps organisations keep information assets secure.

ISO 27000 requires companies to govern and disclose IT as follows (Calder, 2013):

- IT policies and objectives of the company should be considered in relation to the strategic direction of the organisation.

- A framework should be established that clearly sets the objectives of the company and demonstrates the commitment of the company to meet them.
- An IT risk assessment analysis process should exist that analyse the realistic likelihood and potential consequences of IT-related risks and that rank the risks determined.
- Information about technical vulnerabilities should be obtained and appropriate measures should be taken to address the risks.
- The policies and agreements to maintain the security of IT should be transferred within and outside the organisation.

3. METHODOLOGY

The philosophical perspectives used in this study are positivist, interpretivist, and critical postmodernist, as these are the popular paradigms in organisational and management research (Thomas, 2010). A qualitative research approach was followed in order to analyse IT governance through comparison of selected regulations. The selected regulations were confined to King III, as well as international regulations: SOX and ISO. These regulations are submitted to provide comparable, international criteria to evaluate King III IT governance requirements against, due to the following:

- King III was selected as all South African companies are encouraged to comply therewith, and all listed entities are obligated to comply.
- SOX was selected as it is an internationally acclaimed regulation, governing the United States of America (USA) and four of the great eight (G8) countries (Canada, France, Germany, Italy, Japan, Russia, the United Kingdom (UK) and the USA).
- ISO was selected as it is an international, independent non-governmental standard.
- SOX and ISO are applied in developed economies where maturity of IT governance has partly been established (Aydin & Ulger, 2016), and is therefore suitable for comparison against King III IT governance requirements.

4. COMPARISON, FINDINGS AND INTERPRETATION

Proper IT governance has become the absolute expectation of management by companies' stakeholders. Therefore an overview of the IT governance regulations to be evaluated against King III was provided. Table 1 presents a comparison

Vol 8, No 2, 2016 ISSN: 2146-0744 (Online

between King III, SOX and ISO to determine King III's competitive advantage and effectiveness in terms of IT governance.

Table 1 (column one) is a compilation of the requirements according to the different regulations associated with IT governance. All IT governance requirements of King III were selected, and thereafter the requirements of the international regulations (SOX and ISO) were added. Only the requirements not previously included in the table, were added, explaining why not all requirements of all three regulations are displayed.

Table 1: Comparison of King III with international IT governance regulations

Requirements as per Regulation	**KING III (IODSA, 2009)**	**SOX (Stults, 2004 & Correlog, 2011)**	**ISO (BSI 2013)**
The Board of Directors is responsible for IT governance (IODSA, 2009).	√	X	X
IT has been aligned with the performance and sustainability objectives of the company (IODSA, 2009).	√	√	√
The Board of Directors should delegate to management the responsibility of the implementation of an IT governance framework (IODSA, 2009).	√	X	√
The Board of Directors monitors and evaluates significant IT investments and expenditure (IODSA, 2009)[1].	√	X	X
IT is an integral part of the company's risk management (IODSA, 2009).	√	√	√
The Board of Directors ensures that information assets are managed effectively (IODSA, 2009).	√	X	X
A risk committee and audit committee assists the Board of Directors in carrying out its IT responsibilities (IODSA, 2009).	√	√	X
Safeguards are established to prevent data tampering (Correlog, 2011).	X	√	X
Safeguards are established to ensure the effectiveness of the IT controls (Correlog, 2011).	√	√	√
Verifiable controls are established to track data access (Correlog, 2011).	X	√	X

[1] The international regulations do not indicate the party responsible for monitoring and evaluating the company's IT investments, but it does state that the IT investments and expenditures should be governed and disclosed.

Requirements as per Regulation	KING III (IODSA, 2009)	SOX (Stults, 2004 & Correlog, 2011)	ISO (BSI 2013)
IT risk assessment analysis processes are established that assesses the realistic likelihood and potential consequences of IT-related risks and have levels that rank the risks determined (BSI, 2013)[2].	X	X	√
Information about technical vulnerabilities is obtained and appropriate measures are taken to address the risks (BSI, 2013).	√	√	√
The policies and agreements to maintain the security of IT are transferred within and outside the organisation (BSI, 2013).	X	√	√
Number of requirements specifically addressed	**9/13**	**8/13**	**7/13**
Percentage of requirements specifically addressed	**70%**	**62%**	**54%**

Table 1 indicate that King III IT governance meets most of the international IT governance requirements, and leads on an international as it includes most of the local and international IT governance requirements when compared to SOX and ISO.

Some of the requirements stated in the international regulations were, however, not specifically addressed by King III, which follows as suggestions for further improvement of King III IT governance requirements.

5. CONCLUSION AND RECOMMENDATIONS

The study emphasised the importance of IT as part of current corporations' operations. The constant evolving nature of technology increases the usefulness of IT in companies, but also introduces IT-related risks. IT therefore forms an essential part of entities' corporate governance, which is regulated internationally.

The research conducted in this study aimed to determine the international standing of King III IT governance. To determine King III and international IT governance requirements, two international regulations concerning IT governance were reviewed (SOX and ISO). The comparison conducted revealed that King III compares favourably to international regulations with regards to IT governance as it includes most of the international IT governance requirements.

[2] King III and SOX require the companies to manage the risks, but do not specify whether these risks should be measured and ranked.

The comparison performed, however, identified areas where King III IT governance may fall short, and it is proposed that these be added to further improve the IT governance requirements of King III: (i) establish safeguards to prevent data tampering; (ii) establish verifiable controls to track data access; (iii) have an IT risk assessment analysis process which assesses the realistic likelihood and potential consequences of IT-related risks and has levels that rank the determined risks; and (iv) disclose policies and agreements to maintain the security of IT and these policies should be transferred within and outside the organisation.

It is, however, acknowledged that King III provides IT governance principles, and not specific rules, and the omitted requirements are potentially included within the general principles. Also, King IV is currently under development, which may address these shortcomings.

The study was limited to three selected international regulations regarding IT governance: King III, SOX and ISO. Further studies could broaden the selection of international IT governance regulations and evaluate the compliance therewith. Research could also compare King III's requirements, other than IT governance, to relevant international regulations. Finally, in anticipation of King IV, future studies could evaluate King IV's international stance.

REFERENCE LIST

Aydin, M.N. & Ulger, C. (2016), "Perception of IT Governance in an Emerging Market", *International Journal of Computer and Information Technology*, 5(1):1-9.

Brisebois, R., Boyd, G. & Shadid, Z. (2009), "What is IT Governance? And why is it important for the IS Auditor". Toronto: INTO IT.

BSI (2013), *ISO/IEC 27001 Information Security Management System: Self-assessment Questionnaire*, http://www.bsigroup.com/localfiles/en-gb/iso-iec-27001/resources/bsi-isoiec27001-assessment-checklist-uk-en.pdf, [Accessed 23.09.2015]

Butler, R. & Butler, M.J. (2010), "Beyond King III. Assigning Accountability for IT Governance in South African Enterprises", *South African Journal of Business Management*, 41(3):33-45.

Calder, A. (2013), "Information Security and ISO 27001: An Introduction", *IT Governance Green Paper*, Feb.

Coetzee, G.P., Du Bruyn, R., Fourie, H. and Plant, K. (2010), Advanced Internal Audit Topics, 1st ed, Pretoria: Joyprint.

Correlog. (2011), *Sarbanes- Oxley (SOX) Compliance Checklist*, https://correlog.com/support-public/SOX-Compliance.pdf, [Accessed 22.06.2015]

Du Plessis, R. (2009), *Quick Guide to Corporate Governance and King III*, http://services.bowman.co.za/Brochures/OnlineServices/CorporateGovernance/Corporate-Governance-King-3.pdf, [Accessed 03.10.2015]

Grant, K., Hackney, R. and Edgar, D. (2010), Strategic Information Systems Management, China: RR Donelley.

Guldentops, E. (2001), "Asking the Right Questions for IT Governance", *Information Systems Control Journal*, 4(1):13–15.

Hall, J.A. (2011), Information Technology Auditing, 3rd International ed, Australia: South-Western Cengage Learning.

HG.org. (2012), *Information Technology Law: What is Information Technology Law?*, http://www.hg.org/information-technology-law.html, [Accessed 17.09.2015]

Hoekstra, A., Rajkaran, B. and Laubscher, R. (2012), *Chapter 5: The governance of information technology* http://www.pwc.co.za/en/king3/the-governance-of-information-technology/index.jhtml, [Accessed 29.04.2015]

IBM (2011), *Supporting information technology risk management*, https://www-935.ibm.com/services/multimedia/Supporting_Info_Technology_Risk_Mgmnt.pdf, [Accessed 24.02.2015]

IODSA (Institute of Directors in South Africa) (2009), *King Code on Governance Principles for South Africa 2009*, https://c.ymcdn.com/sites/www.iodsa.co.za/resource/collection/94445006-4F18-4335-B7FB-7F5A8B23FB3F/King_III_Code_for_Governance_Principles_.pdf, [Accessed 03.10.2015]

ISACA (Information Systems Audit and Control Association) (2009), *The Risk IT Framework Excerpt: Risk IT based on COBIT*, http://www.isaca.org/knowledge-center/research/documents/risk-it-framework-excerpt_fmk_eng_0109.pdf, [Accessed 03.10.2015]

ISACA (Information Systems Audit and Control Association) (2012), *COBIT 5 Executive Summary*, https://www.isaca.org/COBIT/Documents/Executive-Summary.pdf, [Accessed 18.09.2015]

Leedy, P.D. and Ormrod, J.E. (2014), Practical Research Planning and Design, 10th ed, England: Pearson.

Loebbecke, J.K., Loebbecke, A. and Arens, A.A. (2000), Auditing an Integrated Approach, 8th ed, Upper Saddle River, NJ: Prentice Hall.

Mar, S., Johannessen, R., Coates, S., Wegrzynowicz, K. and Andreesen, T. (2012), *Global Technology Audit Guide: Information Technology Risk and Controls, 2nd ed,* http://www.theiia.org/bookstore/downloads/freetomembers/0_1006.dl_gtag1%202nded.pdf, [Accessed 03.10.2015]

Markus, M.L., Bui, Q.N., Jacobson, D.D., Lisein, O. and Mentzer, K. (2014), The Art of the States. IT Governance and Organizational Performance in American State Governments: Bentley University.

Marx, B. (2009), "An Analysis of Audit Committee Responsibilities and Disclosure Practices at Large Listed Companies in South Africa", *SA Journal of Accounting Research*, 23(1):31-44.

Mizoguchi, T. (2012), *Information Technology Risks in Today's Environment,https://chapters.theiia.org/san-diego/Documents/Seminars/SD_IIA___ISACA_Event_041112_Deloitte_IA_Top_Ten_Risks.pdf,* [Accessed 03.10.2015]

Morikawa, M. and Morrison, J. (2004), *Who Develops ISO standards? A Survey of Participation in ISO, International Standards Development Processes,* http://www.pacinst.org/wp-content/uploads/sites/21/2013/02/iso_participation_study3.pdf, [Accessed 22.04.2015]

National Computing Centre (2005), IT Governance and Developing a Successful Governance Strategy: A Best Practice Guide for Decision Making in IT, Manchester: NCC.

Nkonki (2011), *Integrated Reporting Checklist*, https://www.google.co.za/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&cad=rja&uact=8&ved=0CDAQFjAE&url=http%3A%2F%2Fwww.nkonki.com%2Fdownload.php%3Ffilename%3Dadministrator%2Fmedia%2Fuploads%2Ff2778204-dbf5f0d5caeadceec1633a1f32aab1cd.pdf&ei=__ZBVc2dEcKP7AbHh4GgCg&usg=AFQjCNGCSOy8ij8UPO-lIe9jAvQlAIA0Dg&sig2=uonvd7yYr6V4k26zAWG_LQ&bvm=bv.92189499,d.d24, [Accessed 30.04.2015]

Noraini, C.P., Bokolo, A., Rozi, N.H.N. and Masrah, A.A.M. (2015), "Risk Assessment of IT Governance: A Systematic Literature Review", *Journal of Theoretical and Applied Information Technology*, 17(2):184-193.

Pickett, K.H.S. (2011), The Essential Guide to Internal Auditing, 2nd ed, West Sussex: John Wiley & Sons, Ltd, Publishers.

PwC (PricewaterhouseCoopers) (2015), *King III, IT Governance and Your Organisation*, https://www.pwc.co.za/en/assets/pdf/SteeringPoint-KingIII-IT-Governance-and-KingIII-15.pdf, [Accessed 19.02.2015]

Rao, M. (2003), *Enterprise IT Governance-The obvious step*, http://www.networkmagazineindia.com/200301/cover5.html, [Accessed 13.05.2015]

SOX (2002), *The Sarbanes- Oxley Act of 2002*, http://www.sox-online.com/soxact.html, [Accessed 30.04.2015]

Stults, G. (2004), *An Overview of Sarbanes- Oxley for the Information Security Professional*, http://www.cs.jhu.edu/~rubin/courses/sp06/Reading/soxForInfoSec.pdf, [Accessed 03.10.2015]

Thomas, P.Y. (2010), *Towards Developing a Web-based Blended Learning Environment at the University of Botswana*, Africa, http://uir.unisa.ac.za/handle/10500/4245, [Accessed 30.03.2016]

Tiwana, A., Konsynski, B. and Venkatraman, N. (2013), "Special Issue: Information Technology and Organizational Governance: The IT Governance Cube", *Journal of Management Information Systems*, 30(3):7-12.

Van Grembergen, W. (2013), Introduction to the Minitrack" IT Governance and its Mechanisms"-HICSS 2013, (*In* System Sciences (HICSS), 2013 46th Hawaii International Conference on organised by IEEE).