AN INVESTIGATION INTO INFORMATION SECURITY COMPLIANCE REGULATIONS IN THE SOUTH AFRICAN FINANCIAL SECTOR

Rabbie Maphakela[a], Dalenca Pottas[b], Rossouw von Solms[c]

[a] Department of Information Technology, Nelson Mandela Metropolitan University
[b] Department of Informatics, Nelson Mandela Metropolitan University
[c] Department of Information Technology, Nelson Mandela Metropolitan University

[a] RMaphakela@nmmu.ac.za, +27 41 5043574, PO Box 77000, Port Elizabeth, 6031
[b] Dalenca.Pottas@nmmu.ac.za, +27 41 5049100, PO Box 77000, Port Elizabeth, 6031
[c] Rossouw.VonSolms@nmmu.ac.za, +27 41 5043604, PO Box 77000, Port Elizabeth, 6031

ABSTRACT

As businesses expand more and more into the cyber world, so does the need to secure the information they have. Information security plays a huge role in securing organizational information and also helps to mitigate the probability of threats having an impact on organizational information assets. Furthermore, there are guidelines and standards that help companies to comply with laws or standards that have been created by governmental or other committees. Management have realized the importance of information security and understand their responsibilities towards corporate governance. The problem is that there are various guidelines and standards that make it almost impossible for management to know which guideline and standards to use or leave out. This research focuses on some of the regulations, best practices, standards and guidelines that are of relevance to South African financially oriented institutions. An investigation of different compliance regulations that affect the South African financial sector is made, and common and uncommon elements are identified. Only elements that have an influence in the South African financial sector are identified. The results of the paper will illustrate that a compliance model that incorporates all the guidelines, standards, legislations and best practices for the financial sector is viable.

KEY WORDS

South African Financial Sector, Governance, Information Security, Standards, Guidelines, Compliance

AN INVESTIGATION INTO INFORMATION SECURITY COMPLIANCE REGULATIONS IN THE SOUTH AFRICAN FINANCIAL SECTOR

1 INTRODUCTION

In the past, many companies used to keep their information on paper, which resulted in loss of important information. As businesses expand more and more into the cyber world, so does the need to secure the information they have (Mallela, 2005). Information that is used by companies needs to be protected as it is very critical to the business' productiveness (Thompson et al., 2003). Information security is required to identify security controls that will safeguard the information from threats or attacks. Threats such as hackers or negligence from employees need to be mitigated. Furthermore, the information stored on computers needs to be secured in order to protect the integrity of this information (nCircle, 2005) and from a legal perspective, to avoid being sued by internal or external parties. Corporations are aware of these requirements, but are also aware that there are guidelines that can be used to identify security controls in order to protect the informational assets.

Guidelines, standards, legislations and best practices such as Basel Accord; Sarbanes-Oxley; FICA (Financial Intelligence Centre Act); Banks Act; ECT Act (Electronic Communication and Transaction Act); Gramm-Leach-Bliley Act; and others, have been created to help companies understand their rights and responsibilities among board members, business and IT managers. The problem is that there are various guidelines and standards that make it almost impossible for management to know which guideline and standards to use or leave out.

This research paper focuses on some of the guidelines, legislations and standards that are of relevance to South African financially oriented institutions. An investigation of different compliance regulations that affect the South African financial sector is made, and common and uncommon elements are identified. Only elements that have an influence in the South African financial sector are identified and also the elements that focus more on the security and privacy of financial information. The results of the paper will illustrate that a compliance model that incorporates all the guidelines, standards, legislations and best practices for the financial sector is viable.

2 OVERVIEW OF THE FINANCIAL INDUSTRY

The Financial industry helps a country strengthen its financial systems, grow the economy, restructure and modernize institutions, and respond to the savings and financing needs of all people (Financial Sector, 2005). This is done by providing financing, policy research and advice, and technical support (Financial Sector, 2005). The financial sector is made up of different types of services, namely; banking, mutual funding companies, insurance and other financial service institutions (Macdonald, 1998). Financial sectors deal with information daily, and it is of outmost importance that this information is protected as mentioned before.

It makes good business sense to protect customer information, because it increases the level of confidence in the institution (Federal Trade Commission, 2002). As pointed out before there are guidelines to help with the protection of information through the selection and implementation of security controls. The loss of, or unauthorized access to the information will result in a financial loss to the institution. Therefore, proactive steps must be taken in protecting their financial information, because internal and external attacks are constantly searching for vulnerabilities

(Olson et al, 2005). Attacks such as errors, negligence and hacking are constantly searching for a way to access the information. It is of outmost importance that this information is protected from these attacks (Thompson et al., 2003).

Financial institutions are obliged by the government to protect the financial information. Emerging guidelines, legislation and standards have been created to increase the awareness and understanding of all the risks that organizations may encounter (Olson et al, 2005). This assists with the creation of a secure infrastructure that protects sensitive customer information. Notably, South African financial institutions such as banks are obliged to comply with the Banks Act, before any other regulation, guideline or standard.

The South African banking sector is also affected by more regulatory compliance, since some of the largest banks have expanded internationally to the world's trade markets (Winterboer et al., 2002). Therefore it is important for these leading banks to comply with international standards that affect them. Guidelines, legislation and standard such as the Sarbanes-Oxley Act, which is one of the regulations that banks that go international must also comply with. There are others such as the Basel Capital Accord (Basel II) and the Gramm-Leach-Bliley Act (GLBA) that put emphasis on the privacy on information (MetaGroup, 2005). The South African banking industry has expressed support for standards such as Basel II, and therefore has made important grounds towards compliance.

The next section will focus on and explain some of the guidelines, legislation and standards that are being used in the South African financial sector. The South African financial sector is commonly recognized as world class in terms of its skilled workforce, adequate capital resource, infrastructure and technology, as well as its conducive operating, regulatory environment.

3 GUIDELINES, LEGISLATION AND STANDARDS

Management have realized the importance of information security and understand their responsibilities towards corporate governance (Williams, 2003). However, management needs some form of compliance model that will help them to identify which guidelines affect them as a financial institution and how they can conform to the standards and guidelines and all the relevant laws. The scope of this investigation is limited to:

- The King Report on Corporate Governance for South Africa (King II Report, 2002). The paper uses the King Report as a base for compliance, because it promotes high standards for governance in the context of South African companies.
- The Gramm-Leach-Bliley Financial Services Modernization Act (GLBA). This financial legislation defines financial structure and how to protect financial information (Broaddus, 2000). The GLBA is used in this paper because it is widely used and it affects financial institutions.
- The Sarbanes-Oxley (SOX) is a law that requires firms to certify the integrity of their financial records, their information disclosure controls and internal controls (BSA, 2005). The SOX act is United State oriented and it was selected as it applies to global companies trading in the US.

There are other guidelines, standards legislations and best practices that are of relevance to the South African financial sector and do not resort within the scope of this paper. These include the Financial Intelligence Centre Act, Basel Accord, Banks Act, ECT Act and many more. A brief overview of the afore-mentioned is subsequently provided.

3.1 The Financial Intelligence Centre Act

The Financial Intelligence Centre Act (FICA) mentions that financial institutions cannot execute a transaction with a client that has not been identified (Manuel, 2004). Trevor Manuel (2004) - the South African finance minister - also added that banks and other financial institutions need to know their customers as an important aspect of preventing their institutions from being abused by criminals. In other words customer information needs to be treated with care, caution and be protected from internal or external threats. The FICA promotes customer identification to promote effective money laundering control systems. The Act suggests that reasonable measures be in place to prevent criminals from using false or stolen identities to gain access to financial information and services (Standard Bank, 2005).

3.2 Basel Capital Accord

The Basel Capital Accord (Basel II) becomes effective in 1 January 2007 for banks and December 2006 for other business types. The Basel II attempts to reduce the number of bank failures by binding a bank's capital ratio (ratio of a bank's capital to its total assets) to the riskiness of the loans it makes (Business Report, 2004). All of the major banks have international operations and are governed in compliance with the Basel II. The Basel II is aimed at improving the security and soundness of a financial system (Wilson, 2002).

3.3 Electronic Communication and Transaction Act

The Electronic Communication and Transaction Act (ECT Act) is a South African law that governs electronic activities and aims to reduce the abuse of information systems (ECT, 2002). The ECT Act has an impact on the financial institutions that transact electronically. The ECT Act also focuses on the privacy on information in one of its chapters (Chapter VIII of the ECT, 2002). This chapter focuses on the protection of personal information that is stored, processed or collected electronically. According to Carla Krog (2003) the ECT Act is regarded as a step in the right direction to encourage all South Africans to use the Internet to transact electronically. The ECT Act tries to improve privacy of financial information while transacting electronically.

3.4 Banks Act

The Banks Act is used as a basis for banking services, because it stipulates the requirements for the lawful carrying on of the business of a bank (Banks Act, 1990). This means all the banks have to follow the Banks Act in order to be regarded as a bank, and be allowed to perform banking functions. A bank's functions in the financial services industry includes, carrying out the privilege of currency issue; safeguarding currency stability; helping businesses to develop and providing consumers with the right to withdraw their deposits on demand (Saayman, 2002).

A bank's functions cannot be executed without following certain guidelines, standards and laws. While the scope of this paper is limited to the King report, the GLB act and SOX, it is clear from the overview in Sections 3.1 – 3.4, that there are various other legislations that impact on the operation of financial institutions and the security of financial information. It also serves to confirm the need for a compliance model that will guide institutions towards concomitant compliance with all of the relevant guidelines, legislations and standards.

4 THE KING REPORT

The King Committee on Corporate Governance launched the King Report on Corporate Governance for South Africa – 2002 (King II Report, 2002) at an Institute of Directors (IoD) Conference. The King Report applies to all companies listed on the board of the JSE, such as large public entities, banks, financial and insurance entities (King Report, 2002). The purpose of the King Report is to promote the highest standard of corporate governance for companies. It has been recognized as containing the best governance principles for listed companies in emerging

economies (Dekker, 2005). King II highlights the need for corporate entities in South Africa to move towards a more responsible ethos in corporate governance.

This paper will use the King II as a base standard, because it is a required standard for all the companies listed on the board of the JSE (King Report, 2002). Furthermore, the paper will only focus on the internal audit section of the King Report, as it provides management with reasonable assurance on the effectiveness of internal controls (Dekker, 2005, & King Report, 2002). The other sections of the King Report will not be covered in this paper because they do not focus on the assurance of internal controls and information security.

According to the King Report (2002), the internal audit function should assist executives in maintaining effective controls. This can be done by evaluating those controls to determine their effectiveness and efficiency.

The King Report (2002) recommends that the controls should encompass the following:

- The information systems environment;
- Reliability and integrity of financial and operating information;
- Effectiveness and efficiency of operations;
- Safeguarding of assets; and
- Compliance with laws, regulations and controls
- An effective internal audit function should provide assurance that the management processes are adequate to identify and monitor significant risks.
- Internal audits should be conducted formally at least annually, but more often in more complex organisations.

5 GRAMM-LEACH-BLILEY ACT

The Gramm-Leach-Bliley was signed into law in 1999 by President Bill Clinton (Baker, 2001). It is widely regarded as one of the most significant pieces of federal financial services legislation in many years. The law requires financial institutions to protect the information collected about individuals (Federal Trade Commission, 2005). According to the Federal Trade Commission (2005), the Gramm-Leach-Bliley Act (GLBA) protects consumers' personal information held by financial institutions. The GLBA consists of seven titles and various sections that address affiliation among the financial industry (Moore, 2003). This paper focuses only on the privacy issues in the financial institutions as it deals with the protection of financial information. The other sections of the GLBA will not be used in this paper, because they do not focus on the privacy issues of financial information that are relevant to this paper.

J. A. Broaddus Jnr. (2000) discusses three elements of GLBA, and one of them is to establish the right of customers to protect the privacy of their personal information. One of GLBA's sections called Title V, deals with the privacy issues of information held by financial institutions. The Title V of the GLBA includes a sub-section named 'The protection of non-public personal information' (Moore, 2003). Non-public personal information refers to the information that an individual enters on an application, or information about a transaction between individuals and a company. This section that deals with privacy issues is also known as Section 501.

Section 501, of the GLBA, deals with the Information Security Department of a financial institution and it plays an important role in the compliance with the GLBA. It ensures protection of unauthorized access and anticipated threats to security or integrity. According to Farm9 (2004), Section 501 requires the financial industry to protect the customer's information against unauthorized access that could result in substantial harm or inconvenience to any customer.

In recent years the financial industry was not formally adopted to a set of security standards for achieving GLBA compliance (Moore, 2003). The list below shows some of the requirements for compliance with the GLBA for financial institutions with regards to the protection of unauthorised access, threats to security or integrity (Baker, 2001, Federal Trade Commission, 2005, Federal Trade Commission, 2002 & Moore, 2003):

- A financial institute must provide an initial privacy notice to customers not later than the time the relationship commences.
- Must provide clear and obvious notices of its privacy policies and practices at least annually for the duration of the customer relationship.
- Privacy notice must include accurate statements of company's privacy practices.
- Privacy notice should include what information the company collects and with whom it shares the information.
- If the financial institution wants to disclose information in a way not described on its privacy policy, a revised privacy policy may be required.
- Notices must be provided in a manner so that consumers can reasonably be expected to receive actual notice in writing or electronically, if the consumer agrees.
- Consumers and customers have the right to "say no" to having their information shared with certain third parties.
- Dispose of customer information in a secure manner.
- Wherever possible, minimize the amount of personal data given to commercial or governmental entities. Do not release contact information where it is unnecessary

6 THE SARBANES-OXLEY ACT

The Sarbanes-Oxley Act (SOX) was enacted in 2002 by Congress in the United States, and it affects corporate governance and corporate disclosure (Sophos, 2004). In other words, it is a legislation designed to enhance corporate governance standards (Plotkin, 2003) and identify the responsibilities of executives (CREDANT, 2005). The SOX act is United States oriented, but does apply to global companies trading in the US.

The SOX requires both public and commercial companies to comply with it. It requires public companies to certify to the integrity of their financial records, their information disclosure controls and internal controls (BSA, 2005 & eProject, 2004). The SOX changed the roles and responsibilities of audit and compliance partners of commercial companies. The commercial companies must now consider their financial methods and comply with the new requirements of the SOX (eProject, 2004). Notably, executives are required to sign a confirmation that they are responsible and that the internal controls meet the requirements of SOX (eProject, 2004).

Internal controls are the measures in place to protect assets from threats or attacks. The SOX includes a subsection named Section 404: 'Management Assessment of Internal Controls'. Section 404 requires that each organization's annual report contain an internal control report that will state the responsibilities of management and contain an assessment of internal controls (CREDANT, 2005). This paper will focus on this section as it deals with the securing of financial information, and assurance and reviews of internal controls. However, one of the security standards called 'The Committee of Sponsoring Organizations (COSO) Internal Control – Integrated Framework' has been created to assist companies to comply with SOX. The COSO is a widely accepted standard for organizations implementing and evaluating internal controls in compliance with SOX. Much has

been written about the importance of the Act, but there is little about the influence of IT in this area. Most of the financial reporting requires a well-controlled IT environment to mitigate the risk of threats (IT Governance, 2004).

Usually, in most organizations IT is responsible for the management and control of the systems and technology. Their responsibilities include the collection, storage and management of the data and information contained in the company's financial reports. Management should work closely with the IT Department to determine the financial burdens of storing and preserving the integrity of organizational information (Plotkin, 2003). The IT Department can aid to comply with SOX to protect internal controls (Ruzbacki, 2005). The list below shows some of the requirements for compliance with the SOX (Breisacher, 2004) that are stated in the Section 404 of the SOX:

- Data must be retrievable after long term-retention, even as new technologies are introduced.
- Location where the media is stored must be highly controlled.
- Document any attempt of alteration or deletion of stored information.
- Select tape drives and media with the highest reliability ratings to avoid lack of reliability.
- A consolidated checklist/schedule can be developed to enable financial organizations to identify bottlenecks, shift and balance activities, as well as eliminate inefficiencies.
- Rehearsals and reviews on a regular basis are necessary to ensure that plans are continuing to meet compliance objectives.

According to Christopher Koch (2004), the control report that needs to be produced must include the following:

- A statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting.
- Management's assessment of the effectiveness of the company's internal control over financial reporting.
- A statement identifying the framework used by management to evaluate the effectiveness of the company's internal control over financial reporting.
- A statement that the registered public accounting firm that audited the company's financial statements has issued an attestation report on management's assessment of the company's internal control over financial reporting.

7 FINANCIAL SECTOR COMPLIANCE AND REGULATIONS MODEL

The previous sections provided a brief overview of three of the legislations that are relevant to the South African financial sector. This section will identify elements that are common to each of these regulations and conversely, the ones that are unique to each one of the three laws. Common elements can be identified among the three laws that were investigated in this paper. Therefore, instead of repeating the same elements and re-mentioning what needs to be done, these elements should be combined together and distinctively arranged to avoid redundancy.

In the context of this paper, common elements found in the SOX; GLBA and the King Report, have been grouped under the headings protection and privacy of information and the identification and review of internal controls and the assurance reporting of internal controls to executives or management. The following table (*Table 1. Common issues addressed in the GLBA, SOX and King Report*) shows a summary of common compliance requirements for the identified sections of the

three regulations under discussion. In addition, the second table (*Table 2. Important issues unique to each of the regulations*) lists the elements that are not common to the three laws.

Table 1. Common issues addressed in the GLBA, SOX and King Report

Privacy and Protection	**Identification, reviews and assurance reporting of Internal controls**
1. Safeguarding of assets 2. Assurance on the effectiveness and efficiency of operations within the organization 3. A financial institute must provide an initial privacy notice to customers not later than the time the relationship commences. 4. Location where the media is stored must be highly controlled. 5. Ensure the security and confidentiality of customer non-public information 6. Protect against any anticipated threats or hazards to the security or integrity of sensitive information. 7. Protect against unauthorized access to, or use of, sensitive information.	1. A statement of management's responsibility is needed for establishing and maintaining adequate internal control over financial reporting. 2. A statement is needed for identifying the framework used by management to evaluate the effectiveness of the company's internal control over financial reporting. 3. Rehearsals and reviews on a regular basis are necessary to ensure that plans are continuing to meet compliance objectives 4. Assurance on the effectiveness and efficiency of operations within the organization needs to be completed. 5. External auditor must attest the effectiveness of internal controls each year, based on reliable evidence 6. The directors have a responsibility to ensure that an effective internal control is being maintained

The table (*Table 1*) did not focus on all the elements of the SOX, King Report and the GLBA, as regulations are being reviewed and renewed daily, monthly or annually. Therefore, it is not viable to state that all the elements have been selected and grouped accordingly. The purpose of the paper was not to provide a complete solution, but an overview of the regulations that can be used in the South African financial sector. The focus was to investigate the regulations that can be used for compliance in the South African financial sector for the security of financial information and to reduce the redundancy of regulatory elements. The table (*Table 1*) consists of compliance elements from all three regulations that have been investigated in this paper. As mentioned before, the elements have been grouped according to what type of compliance issue they are enforcing. Therefore, all the common elements are combined which facilitates a simpler method of complying with regulations, standards, guidelines and best practices. However, the requirements unique to a particular law must still be adhered to and these are listed in Table 2.

Table 2. Important issues unique to each of the regulations

GLBA (1999)	**SOX (2002)**	**KING REPORT (2002)**
1. Consumers and customers have the right to "say no" to having their information shared with certain third parties. 2. Enable centralized management of data protection policies and	1. Data must be retrievable even after long term-retention, even as new technologies are introduced.	1. Reliability and integrity of financial and operating information. 2. Pre- and post-implementation reviews have become a key part

enforcement throughout the financial institution. 3. If the financial institution wants to disclose information in a way not described on its privacy policy, a revised privacy policy may be required. 4. A financial institute must provide an initial privacy notice to customers not later than the time the relationship commences. 5. Review the encryption standards used by the institution. The selection of data to encrypt and the encryption technique and level should be supported by the risk assessment.		of successful implementation on strategies

8 CONCLUSION

With so many regulatory demands being placed on businesses, it is easy for an organization to use guidelines that are irrelevant to their line of business (IT Week, 2005). With the realisation from management about the importance of information security, they still do not know which regulation to use or leave out. This paper focused on and examined three regulations that are relevant to the South African financial sector, and attempted to identify similar and different elements and group them together. Regulatory elements that are relevant for the securing of financial information were the main focus.

The three standards that were examined are the King Report, Sarbanes-Oxley (SOX) and the Gramm-Leach-Bliley Act (GLBA). The paper focused on specific sections of these three regulations as they deal with the protection and privacy of financial information, and the assurance and reviews of internal controls. The focus on the King Report was on the internal audit section, as it provides management with reasonable assurance on the effectiveness of internal controls (Dekker, 2005, & King Report, 2002). Additionally the primary focus on the SOX was on section 404. Section 404, of the SOX, requires that each organization's annual report contain an internal control report that will state the responsibilities of management and contain as assessment of internal controls (CREDANT, 2005). Moreover the paper focused on the GLBA and used section 501 of the act to identify elements that are relevant to the financial sector. Section 501 of the GLBA focuses on the protection of unauthorized access and anticipated threats to security or integrity.

These regulations were used because they represent the financial sector standards and promote a high level of corporate governance among financial institutions, especially in South Africa. The similarities between the three regulations included the focus on the Privacy and Protection of information and the identification, review and assurance of internal controls. However, the paper also combined some of the non-similar elements and grouped them accordingly. They are explained as non-similar because they are not covered in all three the regulations, but still need to be complied with.

The paper has illustrated that it is viable to draft a compliance model highlighting common and unique elements across various laws that affect the financial sector. It is recommended that the project scope be expanded to include all the guidelines, standards, legislations and best practices that are relevant to the financial industry. The output will be a model that provides a roadmap for

concomitant conformance with all guidelines, standards, legislations and best practices in the financial sector in the context of the confidentiality, integrity and availability of financial information.

9 REFEENCES

Baker, B. J., 2001, Overview of the Impact of the Gramm-Leach Bliley Act on Bank Insurance Programs [online]. Available on the internet: http://www.nixonpeabody.com/publications_detail3.asp?Type=P&PAID=51&ID=72&Hot (Sited: 20 Mar. 2005)

Banks Act, 1990 [online]. Available on the internet: http://www.acts.co.za/banks/index.htm (Sited: 27 Mar 2005)

Broaddus Jnr., J. A. 2000, An Overview of the Gramm-Leach-Bliley Act and Brief Remarks on the Economy [online]. Available on the internet: http://www.rich.frb.org/media/speeches/al_broaddus/index.cfm/id=20 (Sited: 16 Mar 2005)

Business Report, 2004, Financial compliance driving IT investment [online] Available on the internet: http://www.busrep.co.za/index.php?fSectionId=561&fArticleId=2288490 (Sited: 23 Mar. 2005)

Business Software Alliance (BSA), Information Security Governance: Towards a Framework for Action [online]. Available on the internet: http://www.cccure.org/Documents/Governance/governance.pdf

Conner, W. F, Coviello, A. W., 2004, Information Security Governance: A call to action [online]. Available on the internet: http://www.cyberpartnership.org/InfoSecGov4_04.pdf (Sited: 09 Mar 2005)

CREDANT Technologies, 2005, SOX, GLB, SB 1386 and Mobile Devices – Are You at Risk for Noncompliance? [online]. Available on the internet: http://www.bitpipe.com/detail/RES/1107364149_56.html (Sited: 15 Mar 2005)

Dekker, C. King Report on Corporate Governance for South Africa 2002 – What it means to you [online]. Available on the internet: http://www.cliffedekker.co.za/literature/corpgov/intaudit.htm (Sited: 23 Mar. 2005)

Electronic Communication Transaction Act (ECTA) (25 0f 2002). Vol.446 Government Gazette, Cape Town 02 August 2002

eProject Inc. 2004, Sarbanes-Oxley White Paper [online]. Available on the internet: http://knowledgestorm.co.nz/ksnz/search/viewabstract/71508/index.jsp?pos=29&referer=SEARCH_RESULTS&trkpg=search_results_researchname (Sited: 17 Mar 2005)

Farm9.com, 2004 [online]. Available on the internet: http://farm9.com/pdf/Financial_Regulations.pdf (Sited: 15 Mar 2005)

Federal Trade Commission, In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act [online]. Available on the internet: http://www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.htm (Sited: 15 Mar 2005)

Federal Trade Commission, 2002, Financial Institutions and Customer Data: Complying with Safeguarding Rule [online]. Available on the internet: http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm (Sited: 27 Mar 2005)

Financial Sector, Financial Sector Development [online]. Available on the internet: http://wbln0018.worldbank.org/html/FinancialSectorWeb.nsf/generaldescription/1Financial+Sector+Development?opendocument (Sited: 20 Mar. 2005)

IT Governance Institute, 2004, IT Control Objectives for Sarbanes-Oxley [online]. Available on the internet: http://www.itgi.org/Template_ITGI.cfm?Section=ITGI&CONTENTID=9757&TEMPLATE=/ContentManagement/ContentDisplay.cfm (Sited: 8 Feb 2005)

King Report, 2002, King Report on Corporate Governance for South Africa, Date: 2002

Koch, C. 2004, The Sarbox Conspiracy, Sarbanes-Oxley compliance efforts are eating up CIO time and budgets. Worse, CIOs are being relegated to a purely tactical role. And that may be the CFO's plan [online]. Available on the internet: http://www.cio.com/archive/070104/sarbox.html (Sited: 18 Mar 2005)

Krog, C. 2003, Legislation – Effective e-Commerce [online]. Available on the internet: http://www.vnh.co.za/news_legal_view?mode=content&id=17497 (Sited: 22 Apr 2005)

Macdonald, G. 1998, SkyDome's sibling rivalry [online]. Available on the internet: http://members.fortunecity.com/no_yards/rdome_April_4__1998.htm (Sited: 27 Mar. 2005)

Mallela, S. R. Network Magazine, Security at the top of the Agenda [online]. Available on the internet: http://www.networkmagazineindia.com/200502/coverstory04.shtml (Sited: 09 Mar 2005)

Manuel, T. 2004, Banks may get more time to identify clients [online]. Available on the internet: http://www.iol.co.za/index.php?set_id=1&click_id=13&art_id=qw1086942601651B215 (Sited: 23 Mar 2005)

MetaGroup. 2005, Unraveling Security and Risk Regulation [online]. Available on the internet: http://ww2.websense.com/docs/WhitePapers/Unraveling_Security_and_Risk_Regulation.pdf (Sited: 26 Mar 2005)

Monash, C.A. 2004, The Real Risk [online]. Available on the internet:http://www.computerworld.com/securitytopics/security/story/0,10801,94550,00.html (Sited: 25 Jul 2004)

Moore, M. 2003, Information Security Guide for Gramm-Leach-Bliley Compliance [online]. Available on the internet: http://www.giac.org/certified_professionals/practicals/gsec/3355.php (Sited: 19 Mar. 2005)

nCircle. Implementing Security Best Practices For Sarbanes-Oxley Compliance [online]. Available on the internet: http://www.ncircle.com/pdf/papers/nCircle_WhitePaper_SOA.pdf (Sited: 11 Mar 2005)

Thomson, K., von Solms, R. (2003) Integrating Information Security into Corporate Governance, Presented at: IFIP/Sec2003, Athens, Greece, May 2003

Olson, J., Reymann, P.R. (2005), Proactive Protection of Sensitive Information for Financial Institutions [online]. Available on the internet: http://knowledgestorm.co.uk/shared/write/collateral/WTP/50758_76115_75614_Vormetric_Proactive_Protection_of_Sensitive_Info_04110402-11-2005-12-34-02-PM.pdf (Sited: 27 Mar. 2005)

Plotkin, J. 2003, Corporate Governance – The Impact on Your IT Staff [online]. Available on the internet: http://www.kvsinc.com/_filelib/FileCabinet/PDFs/white%20papers/KVS%20WP%20Plotkin%20Corporate%20Governance.pdf (Sited: 14 Feb 2005)

Ruzbacki, T. Sarbanes-Oxley, IT Governance and Enterprise Change Management [online]. Available on the internet: http://www.mks.com/downloads/SOX_Cobit1.pdf (Sited: 14 Feb 2005)

Saayman, A. 2002, Securitisation as a liquidity source for small banks in South Africa – Chapter 2 [online]. Available on the internet: http://www.ekon-oom.com/andrea/Chapter2.pdf (Sited: 27 Mar. 2005)

Sophos. 2004, Information control with Sarbanes-Oxley: Is your business compliant [online]. Available on the internet: http://www.sophos.com/whitepapers/Sophos-SOX-wpus.pdf (Sited: 15 Mar 2005)

Standard Bank. Financial Intelligence Centre Act – Overview [online]. Available on the internet: http://www.standardbank.co.za/SBIC/Frontdoor_02_02/0,2454,3447_8383722_0,00.html (Sited: 19 Mar 2005)

Williams, P. 2003, IT Management: Enterprise & Supply Chain, Board members need to learn more about IT to fulfil their corporate governance duties [online]. Available on the internet: http://www.computerweekly.com/articles/article.asp?liArticleID=119262&liFlavourID=1 (Sited: 15 Feb 2005)

Wilson, D. 2002, Managing risks critical for Basel II [online]. Available on the internet: http://www.busrep.co.za/index.php?fSectionId=561&fArticleId=124385 (Sited: 23 Mar. 2005)

Winterboer, T., Cloete, J., Malan, H. (2002), PriceWaterhouseCoopers -The Journal, Tackling the key issues in banking and capital markets [online]. Available on the internet: http://www.pwcglobal.com/images/gx/eng/fs/bcm/120202thejournal.pdf (Sited: 18 Mar 2005)

ACKNOWLEDGEMENTS

The financial assistance of National Research Foundation (NRF) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the author and are not necessarily to be attributed to the National Research Foundation.