TOWARDS REGULATORY COMPLIANCE

- A MODEL FOR THE SOUTH AFRICAN FINANCIAL SECTOR –

Rabbie Maphakela[a], Dalenca Pottas[b]

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

[b]Department of Informatics, Nelson Mandela Metropolitan University

[a] RabbieM@korbitec.com, +27 216589700, PO Box 243, Cape Town, 7725

[b] Dalenca.Pottas@nmmu.ac.za, +27 5049100, PO Box 77000, Port Elizabeth, 6031

ABSTRACT

The information age brought along with it, significant advances, challenges and changes, thus resulting in the businesses becoming more complex - significant advances such as using the cyber world as a market place, with the aid of new technology. Clearly, the trend of exploiting the cyber market has benefited the financial industry. However, whereas Information Technology is of critical importance to business, it also creates vulnerabilities which can be exploited.

Many of these security issues are regulated by law. In particular, the SA financial sector is regulated (locally) by the Banks Act, Electronic Communication and Transaction Act (ECT Act) and the Financial Intelligence Center Act (FICA), to name a few. International legislation may also affect local banks, if they have international operations, for example the Gramm-Leach-Bliley Financial Services Modernization Act (GLBA), the Sarbanes-Oxley Act (SOX) and the Basel II Accord.

Undoubtedly, the above-mentioned laws are crucial to ensure inter alia, that the security and privacy of information held by banks are protected. However, the adoption of more and more regulations is drawing heavily on resources from banks that have to ensure compliance with all the relevant laws. Attempts towards compliance might be disjointed and even contradictory if a unified approach is not followed. Various compliance projects initiated by a bank, could also duplicate controls that have already been put in place as part of other projects. Therefore we propose the South African Financial Regulatory (SAFReg) compliance model, a model to facilitate regulatory compliance in the SA financial sector. A generic model is proposed, but elements from the above-mentioned laws that address security and privacy, are used as a case study or proof-of-concept.

KEY WORDS

South African Financial Sector, Information Security, Regulations, Compliance

TOWARDS REGULATORY COMPLIANCE

- A MODEL FOR THE SOUTH AFRICAN FINANCIAL SECTOR –

1 INTRODUCTION

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, n.d.). This is done by providing financing, policy research and advice, and technical support (Financial Sector, n.d.). The financial sector is made up of different types of services, namely; banking, mutual funding companies, insurance and other financial service institutions (Macdonald, 1998).

The information age brought along with it significant advances, challenges and changes, thus resulting in the businesses becoming more complex (Verine, 2004) - significant advances such as using the cyber world as a market place, with the aid of new technology. Kevin Beaver (2003) states that these changes enhance financial services for customers and employees while lowering the overall information technology costs for the financial industry, but increases the security vulnerabilities. Information technology is of critical importance to business, but it also creates vulnerabilities which can be exploited.

Many of these security issues are regulated by law. The SA financial sector is regulated (locally) by the Banks Act, Electronic Communication and Transaction Act (ECT Act) and the Financial Intelligence Center Act (FICA), to name a few (Maphakela, 2005). International legislation may also affect local banks, if they have international operations, for example the Gramm-Leach-Bliley Financial Services Modernization Act (GLBA), the Sarbanes-Oxley Act (SOX) and the Basel II Accord (Maphakela, 2005).

Undoubtedly, the above-mentioned laws are crucial to ensure inter alia, that the security and privacy of information held by banks are protected. However, the adoption of more and more regulations is drawing heavily on resources from banks that have to ensure compliance with all the relevant laws. Attempts towards compliance might be disjointed and even contradictory if a unified approach is not followed. Various compliance projects initiated by a bank, could also duplicate controls that have already been put in place as part of other projects. Therefore we propose the South African Financial Regulatory (SAFReg) compliance model, a model to facilitate regulatory compliance in the SA financial sector. A generic model is proposed, but elements from the above-mentioned laws that address security and privacy, are used as a case study or proof-of-concept.

2 IMPORTANCE OF SECURITY AND THE BROADER FRAMEWORK

As organisations become more profitable and more competitive, they realise the opportunities of the internet (Singh, 2004; Stichele, 2004). New businesses have sprung up on the Internet without a physical presence, because they have seen that greater markets can be achieved (Singh, 2004). The financial industry also got caught in the hype of moving to the cyber world because there is no physical product that needs to be delivered (Singh, 2004), and their customers can be easily swayed to use internet services (Dombi, 2001).

Information security is about protecting companies' assets and processes (Gillespie et al, 2004). Information security aids financial institutions with the securing of financial information by reducing the risk of threats to a minimum. Financial information is regarded as the most important assets for financial services, because it is information about their customers (Cenzic, 2005).

The financial industry deals with sensitive information on a continuous basis and it is of outmost importance that this information is protected. It makes good business sense to protect

customer information, because it increases the level of confidence in the institution (Federal Trade Commission, 2002). There are threats that are constantly searching for vulnerabilities in systems. Threats that organisations are facing in this technological age can either be internal or external (Gillespie et al, 2004). However, these threats can be alleviated with the aid of regulations that have been compiled by government.

There is a greater need for regulation in the financial services industry, because financial services carry huge amounts of society's cost, and consumers need to feel confident in the service (Falkena et al, 2001). Furthermore, regulations are a first step in addressing problems which arises when organizations disregard the importance of their information (Sophos, 2004). Moreover if anything happens, like a huge disruption, it is easier to keep the business running. The company will continue running through the guidance of regulations used to secure their information.

3 SOUTH AFRICAN LEGISLATIONS

The South African banking sector is also increasingly affected by regulatory compliance, because some of the largest banks have expanded internationally (Winterboer et al., 2002). Therefore it is important for these leading banks to comply with international laws and standards that affect them, as well as the local laws and standards.

For the purpose of this research, the paper focuses only on the security and privacy issues that are relevant in protecting financial information for South African financial institutions. The focus will be on local and international regulations that have an effect on the South African financial sector. These are detailed in Sections 3.1 and 3.2 respectively.

3.1 Local (South African) Regulations

- The King Report on Corporate Governance for South Africa (King II Report, 2002).

  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 paper uses the King Report as a base for compliance, because it promotes high standards for governance in the context of South African companies.

- Financial Intelligence Center Act (FICA)

  FICA 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). The FICA promotes customer identification and the avoidance of money laundering activities (FICA, 2001).

- Electronic Communications and Transaction Act (ECT Act)

  The ECT Act is a South African law that governs electronic activities and aims to reduce the abuse of information systems (ECTA, 2002). The ECT Act has an impact on the financial institutions that transact electronically.

- 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.

3.2 International Regulations

- 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 Act (SOX)

  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 States-oriented and it was selected as it applies to global companies trading in the US.

- BASEL Accord (Basel II)

  The BASEL Accord is aimed at improving the security and soundness of a financial system (Wilson, 2002). All of the major banks that have international operations are governed in compliance with the Basel II.

4 THE PROPOSED COMPLIANCE MODEL

An increasing number of regulations are imposed on companies, including South African Banks. Adding to the trouble is that the requirements of most regulations often overlap extensively, leaving organizations with the challenge of sorting out which solutions meet which requirements of which regulations (IDC, 2005) – therefore the IDC believes that it will be increasingly important for businesses to find ways to manage the mapping and identification of requirements into easily deployable security policy. The Australian Government also states that a compliance model promotes a hierarchical approach to compliance improvement (Australian Government, 2005).

Therefore this paper proposes the South African Financial Regulatory compliance (SAFReg) model to solve these problems, viz facilitating a hierarchical approach to regulatory compliance and getting rid of unnecessary overlapping requirements as contained in the various legislations.

The SAFReg model consists of four phases that will/can be used to comply with the regulatory pressures from governmental regulations. The four phases (as illustrated in Figure 1) are:

1. Regulation identification
2. Identification of sections relevant to the securing of information
3. Assessment of sections (to identify common and unique elements)
4. Compilation of elements into a regulatory compliance model

The benefits derived from the application of such a compliance model, include:

- A framework to manage compliance with multiple regulations.
- Optimization of resources – less time, money and people are required to implement and maintain a unified compliance approach
- Elimination of redundancies found in various legislations.
- Reduction in overall compliance monitoring efforts

The SAFReg model is comprised by four phases as mentioned above. These phases are discussed in Section 5.

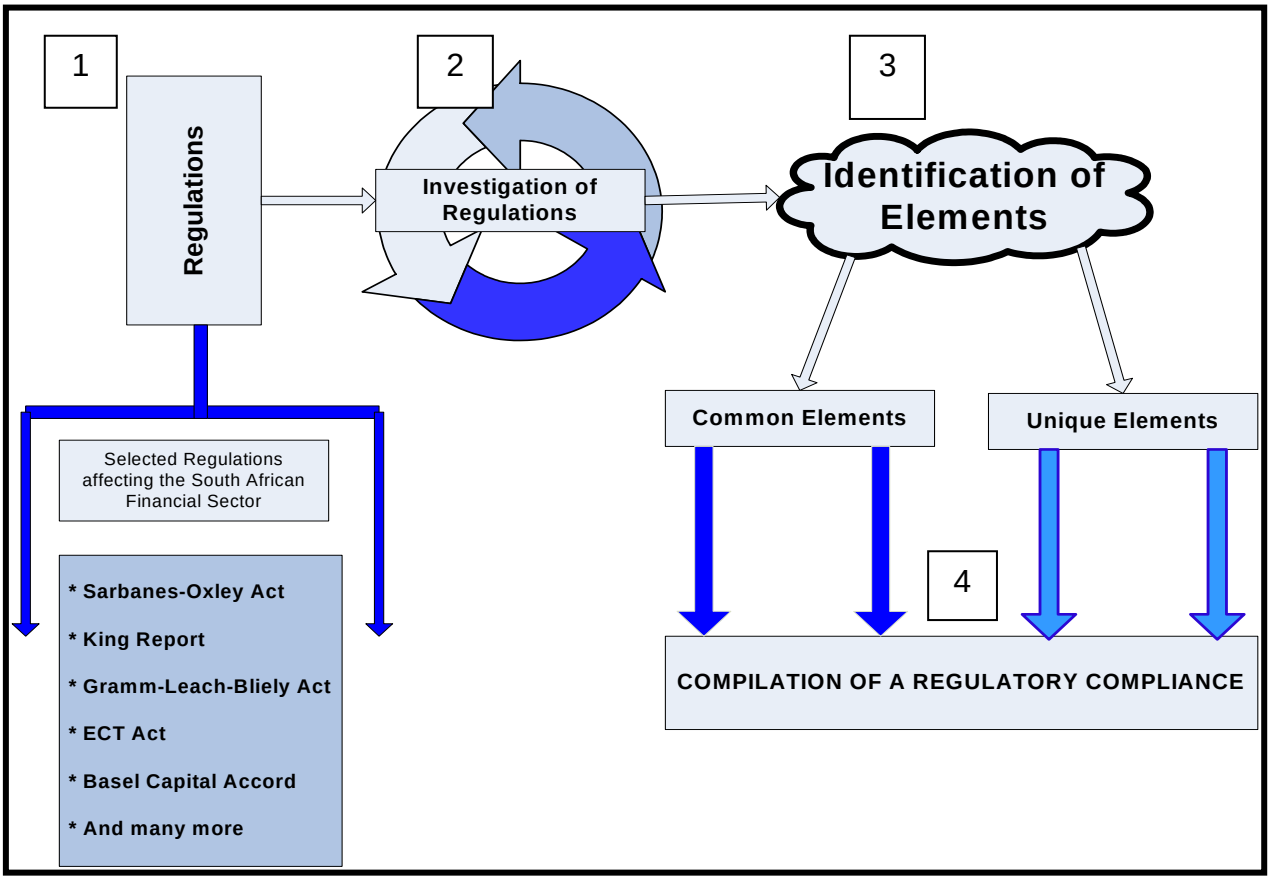

Figure 1: The South African Financial Regulatory Compliance (SAFReg) model

5 PHASES OF THE SAFREG MODEL

Consider a typical financial institution (Bank-X) who has to comply with the regulations enumerated in Sections 3.1 and 3.2. The following sections expound on the actions required as part of each of the four phases of the SAFReg model.

5.1 Phase 1: Regulation Identification

This first phase of the model deals with the identification of regulations that are affecting the South African financial sector. As stated previously, there are various regulations and not all regulations affect all types of institutions. This phase is a process whereby resources will be allocated by the organisation to identify the regulations that affect the organisation.

The result of this process is a list of the regulations that affect Bank-X. In this case and for the purpose of this paper, the list will include the regulations mentioned in Section 3.

5.2 Phase 2: Identification of Sections relevant to the securing of information

Moving to the second phase of the model, the next requirement is the identification of sections included in the regulations, which affect the security and privacy of information. This phase is a process of reviewing each regulation and identifying the sections that are relevant to the protection or securing of information (in this regard financial information).

As regarding Bank-X, the various sections from the relevant regulations have been identified and are listed in the following table (Table 1).

Table 1: Regulations and the sections that focus on securing information

Regulation Name	**Section to be used for securing information**
King Report	Section 2 - Risk Management
Basel Accord	Part 4: The Third Pillar – Market Discipline
Gramm-Leach-Bliley Act	Section 501
Sarbanes-Oxley Act	Section 404
Financial Intelligence Center Act	All the Sections
Banks Act	All the Sections
ECT Act	Chapter VIII

5.3 Phase 3: Assessment of Sections

The third phase of the model is a continuous process which requires an intense assessment of the sections detailed in Table 1. It deals with the process of identifying elements which are common and those which are unique to each of the regulations. This phase is constituted as follows:

5.3.1 Review Elements

List all the elements from the section that deals with the securing of information.

5.3.2 Identify Category

Categorize each element according to “privacy issues” or “internal controls”. Note that this categorization was used for the purpose of this paper to categorize common elements found in the various legislations.

5.3.3 Compare (elements to each other)

Now compare the elements with each other to check whether they are already being handled by another element from another regulation or not.

The result of this phase is illustrated in Figure 2.

5.4 Phase 4: Compilation of elements into a regulatory compliance model

Lastly, Phase 4 of the model deals with the implementation of the elements identified during Phase 3. This phase takes as input the common and unique elements identified during Phase 3. The identified elements can be compiled into a document or preferably a database to facilitate future reference and maintenance.

Bank-X is now at a stage where solutions can be implemented to ensure compliance with the various legislations. However, it is important that this does not become a “knee-jerk” reaction to comply at all costs – thereby ending up with multiple and potentially redundant solutions, without a clear cost benefit, that are often a source of consternation (IDC, 2005).

This phase requires diligent mapping of the requirements (elements) to solutions while keeping tabs to ensure that the selected or envisaged solution(s) satisfies the requirements of all the regulations.

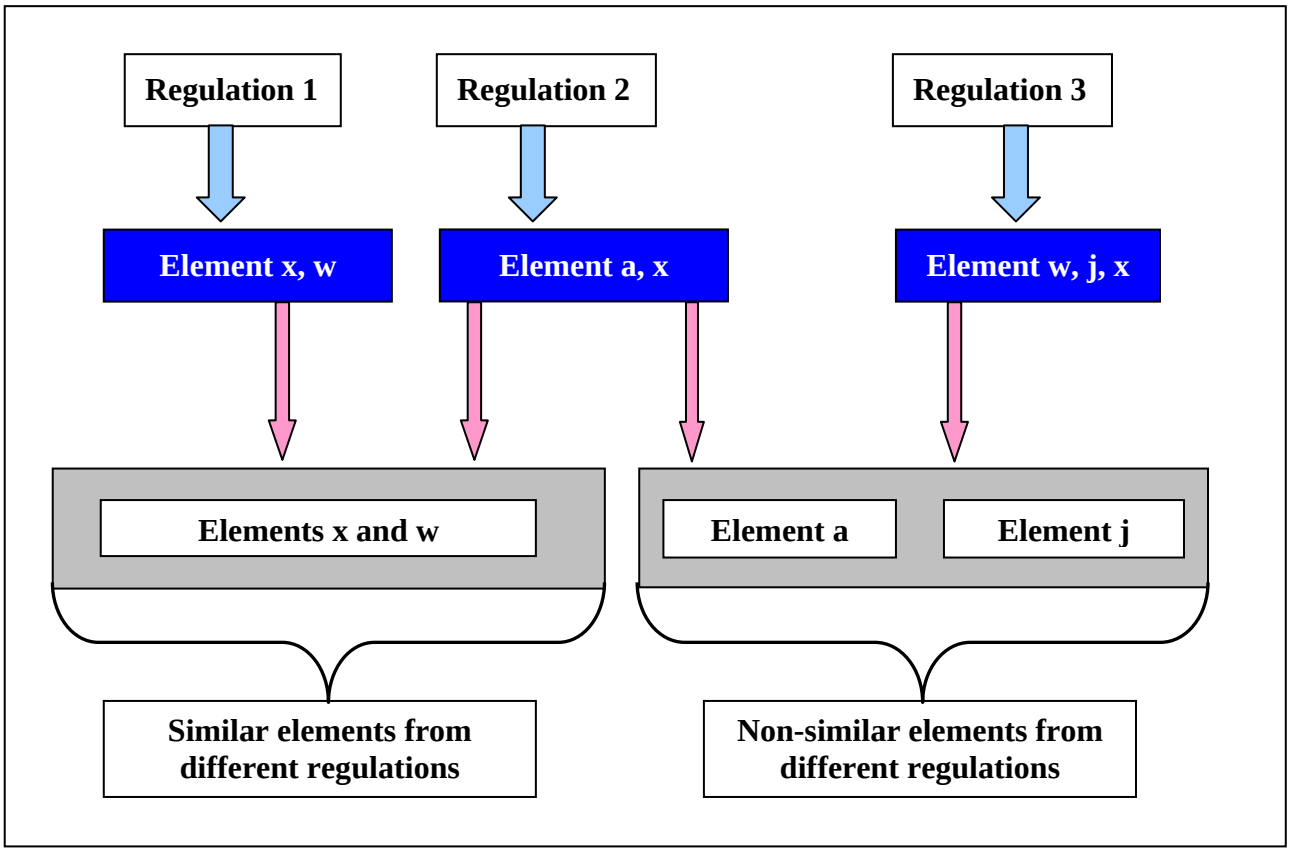

Figure 2: Assessment of regulations and sections from different litigations

5.5 Outcome of the results

The usage of the compliance model has resulted in the identification of common elements that have been combined together and distinctively arranged to avoid redundancy. However, there are also unique elements that are not similar or found in other regulations.

The following table (*Table 2: Common issues found in regulations that affect Bank-X*) shows a summary of requirements for the identified sections of the regulations that affect Bank-X. In addition, the second table (*Table 3: Important issues unique to international regulations that affect Bank-X*) and the third table (*Table 4: Important issues unique to local regulations that affect Bank-X)* show a summary of elements unique to the international and local regulations respectively.

Note that the tables did not focus on all the elements of the selected regulations and that it is not viable to state all the elements that have been selected and grouped accordingly. The purpose of the paper is not to provide a complete solution, but to show the viability and necessity of following a unifying compliance model, rather than ad hoc, randomized compliance projects.

Table 2: Common issues found in regulations that affect Bank-X

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	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

Privacy and Protection	Identification, reviews and assurance reporting of internal controls
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.	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

Table 3: Important issues unique to international regulations that affect Bank-X

GLBA (1999)	SOX (2002)	BASEL II
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 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	1. Data must be retrievable even after long term-retention, even as new technologies are introduced.	1. Information relating to the financial position, performance, corporate governance, risk management and risk exposure of a listed company should be transparent and reliable. 2. Banks should have an approach for determining what disclosures it will make and the internal controls over the disclosure process.

GLBA (1999)	SOX (2002)	BASEL II
level should be supported by the risk assessment.		

Table 4: Important issues unique to local regulations that affect Bank-X

KING REPORT (2002)	FICA (2001)	ECT ACT (2002)	BANKS ACT (1990)
1. Reliability and integrity of financial and operating information. 2. Pre- and post-implementation reviews have become a key part of successful implementation on strategies	1. Identify and verify clients 2. Record all business relations and transactions. 3. Report suspicious and unusual transactions.	1. Only deal with data collectors that have subscribed to the recorded data protection principles 2. Consumer information needs to be provided in order to identify and validate the consumer. 3. Consumers have the right not to be bound to unwanted communications offering goods or services (spam). 4. If the consumer is bounded, then they must have the option to cancel the subscription to the mailing list. 5. The supplier's payment system must be sufficiently secure and the supplier will be liable for any damage due to damage to the payment system or consumer information	1. Provides information for banks to follow in order to be regarded as a bank, and be allowed to perform banking functions.

6 CONCLUSION

The end of the 20th Century and the start of the 21st saw two events that radically changed the business landscape - corporate champions fell from grace in a series of stunning failures, while the Internet transformed the way governments, companies, and individuals communicate (Getronics, 2005). Both of these events impacted heavily on the financial sector, with legislation imposing strict regulatory requirements on the one hand and the Internet opening up avenues for new business ventures.

Private information held by a financial institutions needs to be managed and secured from any harm that may occur to the information (Maphakela et al, 2005). Regulations have been created to aid financial institutions with ways of controlling security related issues. The backlash of financial scandals and theft of personal and private user and customer data caused a plethora of regulations to spring up worldwide, however, the complexity of these regulations and standards has a significant negative impact on the ability of businesses to implement and comply with them (IDC, 2005).

The South African financial sector is also affected by regulations, both from local and international origin. However, the adoption of more and more regulations is drawing heavily on resources from banks that have to ensure compliance with all the relevant laws. Attempts towards compliance might be disjointed and even contradictory if a unified approach is not followed. Various compliance projects initiated by a bank, could also duplicate controls that have already been put in place as part of other projects. Therefore we propose the South African Financial Regulatory (SAFReg) compliance model, a model to facilitate regulatory compliance in the SA financial sector.

The SAFReg model provides a roadmap for concomitant conformance with legislations affecting the South African financial sector. On a final note, it follows that the model could be expanded to include guidelines, standards and best practices relevant to the financial sector. Such a broader, all-inclusive approach can assist to unify legislative compliance attempts with other projects that focus on implementing security guidelines, standards and best practices.

7 REFERENCES

Australian Government, 2005, Improving Tax Compliance in the Cash Economy: April 1998, Sited: 29 Jul 2005, URL: http://www.ato.gov.au/businesses/content.asp?doc=/content/39073.htm&page=38&H38

Banks Act, 1990, Cited: 27 Mar 2005, URL: http://www.acts.co.za/banks/index.htm

Beaver, K., 2003, Achieving GLBA Compliance for Web Applications Through Security Testing, Sited: 12 Aug 2005, URL: http://www.spidynamics.com/assets/documents/WebInspect_GLBA.pdf

Broaddus Jnr., J. A. 2000, An Overview of the Gramm-Leach-Bliley Act and Brief Remarks on the Economy, Date: 17 Feb 2000, Cited: 16 Mar 2005, URL: http://www.rich.frb.org/media/speeches/al_broaddus/index.cfm/id=20

Business Software Alliance (BSA), n.d, Information Security Governance: Towards a Framework for Action, URL: http://www.cccure.org/Documents/Governance/governance.pdf

Cenzic, 2005, Application Security for Financial Institutions: Under GLBA, FFIEC, and Other Laws, Sited: 23 Jun 2005

Dombi, J., 2001, “Point-and-Click Banking Bliss”, The Muhlenberg Advocate, Vol. 1 no. 3, Sited: 06 Aug 2005, URL: http://www.muhlenbergadvocate.com/archives/v1i3/articles/banking2.htm

Electronic Communication and Transaction Act (ECT Act), 2002, Date: Aug 2002, Cited: 14 Mar 2005, URL: http://www.acts.co.za/ect_act/index.htm

Falkena, H., Bamber, R., Llewellyn, D., Store, T., 2001, Financial Regulation in South Africa, Sited: 23 Mar 2005, URL: http://www.finforum.co.za/publications/fregall.pdf

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, n.d, Financial Sector Development, Date unknown, Cited: 20 Mar. 05, URL: http://wbln0018.worldbank.org/html/FinancialSectorWeb.nsf/generaldescription/1Financial+Sector+Development?opendocument

Getronics, 2005, Security Compliance: Practical Strategies to Alleviate Regulatory Frustration, Sited: 23 Apr 2006, URL: http://www.getronics.com/us

Gillespie, P., Rasmussen, M., 2004, Combating Fraud in Financial Services, Sited: 29 Jul 2005.

IDC, 2005, Optimizing Your IT Controls Environment for Compliance with Multiple Regulations.

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

Macdonald, G., 1998, SkyDome's sibling rivalry, Date: 04 Apr. 1998, Cited: 27 Mar. 2005, URL: http://members.fortunecity.com/no_yards/rdome_April_4__1998.htm

Maphakela, R., Pottas, D., von Solms, R., 2005, An Investigation into Information Security Compliance Regulations in the South African Financial Sector, Paper presented at: ISSA Conference 2005, Sandton, Johannesburg, June 2005.

Singh, A., 2004, Trends in South African Banks, Aslib Proceedings: New Information Perspectives, vol. 56, no 2, pp. 187-196.

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, n.d., Financial Intelligence Centre Act – Overview, Date Unknown, Cited: 19 Mar 2005, URL: http://www.standardbank.co.za/SBIC/Frontdoor_02_02/0,2454,3447_8383722_0,00.html

Stichele, M. V., 2004, Critical issues in the Financial Industry, Sited: 06 Aug 2005, URL: http://www.somo.nl/html/paginas/pdf/FS_Report_full_2004_EN.pdf

Verine, E., 2004, Legal implications of information security governance, Sited: URL: http://etd.rau.ac.za/theses/available/etd-08252004-102326/restricted/LLMchapter7.pdf

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)