A Model for Legal Compliance in the South African Banking Sector
- An Information Security Perspective -

by

Rabbie Maphakela
A Model for Legal Compliance in the South African Banking Sector
- An Information Security Perspective -

by
Madidimalo Rabbie Maphakela

DISSERTATION

Submitted in fulfilment of the requirements for the degree

MAGISTER TECHNOLOGIAE

in
Information Technology

at the
School of Information and Communication Technology

in the
FACULTY OF ENGINEERING, THE BUILT ENVIRONMENT AND INFORMATION TECHNOLOGY

of the
NELSON MANDELA METROPOLITAN UNIVERSITY

Supervisor: Prof Dalenca Pottas

January, 2008
DECLARATION BY STUDENT

NAME: MADIDIMALO RABBIE MAPHAKELA

STUDENT NUMBER: 20104543

QUALIFICATION: MAGISTER TECHNOLOGIAE: INFORMATION TECHNOLOGY

TITLE: A MODEL FOR LEGAL COMPLIANCE IN THE SOUTH AFRICAN BANKING SECTOR: AN INFORMATION SECURITY PERSPECTIVE

DECLARATION:

In accordance with Rule G4.6.3, I hereby declare that the above-mentioned treatise/dissertation/thesis is my own work and that it has not previously been submitted for assessment to another University or for another qualification.

SIGNATURE: .........................................

DATE: 28 January 2008
Contents

Abstract vi

1. Chapter 1: Introduction and Background 01
   1.1 Introduction
      1.1.1 Corporations, Fraud and Ethics 01
      1.1.2 Enron 02
      1.1.3 WorldCom 03
      1.1.4 Consequences of Unethical Behaviour 03
   1.2 Information Security 04
   1.3 Corporate, IT and Information Security Governance 06
      1.3.1 Corporate Governance 07
      1.3.2 IT Governance 07
      1.3.3 Information Security Governance 07
   1.4 The Legislative Response 08
      1.4.1 Terminology Defined 08
      1.4.2 Legal Sources 09
   1.5 Problem Statement 11
   1.6 Limitations in Scope 12
   1.7 Objectives of the Study 13
   1.8 Methodology 14
   1.9 Layout of the Dissertation 16
   1.10 Conclusion 18

   2.1 Introduction 19
   2.2 The Financial Industry 21
      2.2.1 Banking 21
      2.2.2 Mutual Funding 23
      2.2.3 Insurance Services 24
   2.3 The Financial Industry and the Shift to Cyber-World 25
2.4 Financial Information and Security
   2.4.1 Importance of Security
   2.4.2 Threats that Affect Organisations
   2.4.3 Security in the Financial Industry
2.5 Internal Controls
   2.5.1 Operational Risk Management and Internal Controls
   2.5.2 Groups of Controls
   2.5.3 Selecting the Right Controls
2.6 Conclusion

3. Chapter 3: Legal Sources

3.1 Introduction
3.2 The Need for Legal Sources within Organisations
3.3 Legal Sources – The Impact on IT Operations in Financial Services
3.4 Legal Sources Affecting the South African Financial Sector
   3.4.1 Local (South African) Legal Sources
      3.4.1.1 The King Report
      3.4.1.2 The Financial Intelligence Centre Act
      3.4.1.3 The Electronic Communications and Transactions Act
      3.4.1.4 The Banks Act
   3.4.2 International Legal Sources
      3.4.2.1 The Gramm-Leach-Bliley Act
      3.4.2.2 The Sarbanes-Oxley Act
      3.4.2.3 The Basel Capital Accord (Basel II)
3.5 Conclusion

4. Chapter 4: A Model for Legal Compliance in the South African Banking Sector

4.1 Introduction
4.2 Why a Compliance Model?
4.3 Proposed Compliance Model and Benefits
4.4 The Phases of the SABS-LeCoM
   4.4.1 Phase 1: Legal Source Identification
   4.4.2 Phase 2: Identification of Sections Relevant to the Issues of
5. Chapter 5: SABS-LeCoM: Proof of Concept Using Privacy and Internal Controls

5.1 Introduction

5.2 SABS-LeCoM – Proof of Concept
   5.2.1 Phase 1: Legal Source Identification
   5.2.2 Phase 2: Identification of Sections Relevant to the Issues of Concern
   5.2.3 Phase 3: Assessment of Sections
      5.2.3.1 Step 3.1: Review Elements
      5.2.3.2 Step 3.2: Identify and Allocate Categories
      5.2.3.3 Step 3.3: Compare Elements
   5.2.4 Phase 4: Implementation of Solutions

5.3 Conclusion

6. Chapter 6: Conclusion

6.1 Introduction

6.2 Benefits of the SABS-LeCoM
   6.2.1 Compliance Management for Multiple Legal Sources
   6.2.2 Optimization of Resources
   6.2.3 Elimination of Redundancies
   6.2.4 Reduction in Overall Compliance Monitoring Effort
   6.2.5 Combination of Effort and Resources Towards Security Initiatives

6.3 Chapter Overview
   6.3.1 Chapter 1 – Introduction
   6.3.2 Chapter 2 – South African Financial Institutions and Financial Information Security
   6.3.3 Chapter 3 – Legal Sources
   6.3.4 Chapter 4 – A Model for Legal Compliance in the South African
Banking Sector 108
6.3.5 Chapter 5 – SABS-LeCoM: Proof of Concept Using Privacy and Internal Controls 109
6.3.6 Chapter 6 – Conclusion 109
6.4 Future Research 110
6.5 Conclusion 111

References 112

Appendix A 127

Tables and Figures

<table>
<thead>
<tr>
<th>Figure/Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 2.1</td>
<td>2002 Market Share of the “Big Four” South African Banks</td>
<td>30</td>
</tr>
<tr>
<td>Figure 2.2</td>
<td>2004 Global Survey Results on the Top Ten Security Concerns for Organisations</td>
<td>39</td>
</tr>
<tr>
<td>Table 3.1</td>
<td>Departments Affected by SOX</td>
<td>66</td>
</tr>
<tr>
<td>Figure 4.1</td>
<td>SABS-LeCoM – A High-Level Diagrammatic Representation</td>
<td>75</td>
</tr>
<tr>
<td>Figure 4.2</td>
<td>Legal Source Identification</td>
<td>77</td>
</tr>
<tr>
<td>Figure 4.3</td>
<td>Investigation of Legal Sources</td>
<td>79</td>
</tr>
<tr>
<td>Figure 4.4</td>
<td>Element identification through the Investigation process</td>
<td>80</td>
</tr>
<tr>
<td>Figure 4.5</td>
<td>Assessment of legal sources, sections and elements</td>
<td>82</td>
</tr>
<tr>
<td>Figure 4.6</td>
<td>Compilation of common and unique elements</td>
<td>83</td>
</tr>
<tr>
<td>Table 5.1</td>
<td>Summary of legal sources identified (Local and International)</td>
<td>87</td>
</tr>
<tr>
<td>Table 5.2</td>
<td>Legal sources and the sections that focus on securing information</td>
<td>90</td>
</tr>
<tr>
<td>Table 5.3</td>
<td>Common issues found in the legal sources that affect Bank-X</td>
<td>103</td>
</tr>
<tr>
<td>Table 5.4</td>
<td>Important issues unique to international legal sources that affect Bank-X</td>
<td>105</td>
</tr>
<tr>
<td>Table 5.5</td>
<td>Important issues unique to local legal sources that affect Bank-X</td>
<td>106</td>
</tr>
<tr>
<td>Table 5.6</td>
<td>Cross-Referencing Compliance Controls with Security Initiatives</td>
<td>108</td>
</tr>
<tr>
<td>Figure 5.1</td>
<td>SABS-LECOM – High-Level Diagrammatic Representation</td>
<td>110</td>
</tr>
</tbody>
</table>
Abstract

In the past, many organisations used to keep their information on paper, which resulted in the loss of important information. In today’s knowledge era the information super-highway facilitates highly connected electronic environments where business applications can communicate on an intra- as well as inter-organizational level. As business expanded more into the cyber-world, so did the need to protect the information they have. Technology advances did not only bring benefits, it also increased the vulnerability of companies’ information. Information, the lifeblood of an organization, must be protected from threats such as hackers and fraud, amongst others.

In the highly regulated financial sector, the protection of information is not only a best practice, but a legal obligation carrying penalties for non-compliance. From a positive aspect, organisations can identify security controls that can help them to secure their information, with the aid of legal sources. But organisations find themselves burdened by a burgeoning number of legal sources and requirements, which require vast resources and often become unmanageable.

This research focuses on finding a solution for South African banks to comply with multiple legal sources, as seen from an information security perspective.
Chapter 1
Introduction and Background

1.1 Introduction

As more business transactions shift from paper-based to electronic record-keeping, risks such as accidental disclosure of information increase. The risk of someone accessing the information is high because business information that is stored on computers can be easily manipulated (Sophos, 2004). The security of information and business ethics also decreases with the transactional shift of information storage. The introduction of the Internet and the eBusiness era in the early 1990s did not help either, as many organisations began pushing to see what they can get away with (Le Grand, 2003), from fraud to inappropriate behaviour. Ethics in business has been an issue for ages, and today there are examples of corporations and individuals who have run into legal and financial trouble due to their doubtful ethics (Stralser, 2004).

1.1.1 Corporations, Fraud and Ethics

Steven Stralser (2004) defined ethics as the moral standards used to judge right from wrong. For organisations, ethics are the standards of moral values and conduct that govern decisions made and actions carried out in the work environment. In other words, decisions made are for the benefit of the organisation instead of benefiting the decision-maker.

The news is filled with organisations’ overstated profits, deceitful accounting practices and the private use of company funds (Sophos, 2004), in other words,
financial statement fraud. Deloitte (n.d.) refers to financial statement fraud as “the deliberate fraud committed by management that injures investors and creditors through materially misleading financial statements”.

Fraud is a key threat to the accuracy and fairness of financial statements, and this was evident with organisations such as Enron and WorldCom (Pasley, 2005). Too many people have lost jobs and retirement savings due to their company’s unethical behaviour. Therefore, with no measures protecting and securing the information, corporate insiders can exploit the weaknesses within the organisation and sabotage company information.

A good example of a company that committed severe ethical violations was Enron Corporation. Enron went bankrupt because the fundamental physical processes of the organisation were failing and the company did not have to report in publicly released financial statements for many periods (Smith, n.d.). The forthcoming sections give a brief background on two famous corporate fraud organisations, Enron and WorldCom, and how they became notorious in the business world.

1.1.2 Enron

As one of the notorious companies that committed serious ethical violations, Enron was one of the largest energy companies in the United States, with over 19 000 employees in 40 countries (Stralser, 2004 & Myburgh, 2003). However, in 2001 it became clear that Enron was involved in a huge accounting scandal and declared bankruptcy (Myburgh, 2003). A large percentage of Enron’s assets were never physically verified in the auditing and financial reporting (Le Grand, 2003).

The Enron board of directors failed to protect the company by allowing it to engage in high-risk accounting, inappropriate conflict of interest transactions and
excessive executive compensation (Myburgh, 2003). The board of directors allowed the conducting of deceptive accounting practices to make the company’s financial condition appear better than it was and to reward themselves with huge amounts of bonuses (Stralser, 2004; Myburgh, 2003; Bloem et al, 2006). At the same time, thousands of employees lost their retirement savings.

1.1.3 WorldCom

In 2002, WorldCom began to unravel the largest financial fraud in the history of the United States (Stralser, 2004). The company officials had misstated accounting figures of large amounts (Myburgh, 2003). Apparently, the problem was discovered during a routine audit, and it was clear that the company expenses were booked as assets. The CEO of WorldCom was granted loans of huge amounts, and that lead to the bankruptcy of the company and the lay-off of thousands of employees (Stralser, 2004). However, WorldCom has changed its name and it currently requires its employees to take ethical courses. The company’s past has resulted in the profound awareness and support for both the concepts and merits of governance (Cohasset Association, 2005).

1.1.4 Consequences of Unethical Behaviour

Unethical behaviour within organisations can result in the downfall of them. As seen with Enron and WorldCom, executives had the authorisation to alter company’s private information for their own benefit. Company information should be secured from unauthorised alteration and access to ensure the integrity of that information; therefore, it follows that information security has an important role to play in prohibiting unethical and illegal behaviour such as transpired at Enron and WorldCom.
1.2 Information Security

As information becomes easy to access using technology, it becomes clear that information needs to be secured, because technology brings along with it more risks for company information. For most businesses, information and technology have been key drivers for their success. IT has helped transform businesses and created opportunities for most organisations. Through the use of IT, organisations have increased the growing dependence on their information systems for their business processes, thereby exposing the business to the threats associated with the electronic processing of information. Nevertheless, organisations that depend on technology to conduct business need to provide evidence that such technology is efficient and securely managed (Le Grand, 2003).

Information security is not a simple topic, thus resulting in disinterest from directors and corporate executives (Loyd, 2004). However, the afore-mentioned financial scandals have contributed greatly to changing executives’ views on the importance of information security. Management and executives are accountable for an organisation’s success, and are, therefore, responsible for the protection of its information (Le Grand, 2003). Management should actively engage in assessing emerging threats and provide strong security leadership for effective corporate security (Conner et al. 2004).

The objective of information security is to protect the interest of those relying on information, and the systems and communications that deliver the information (Gillespie et al, 2004). As information becomes more valuable, it becomes a greater target for theft, fraud and attacks. The information must be protected against harm from threats leading to different types of vulnerabilities such as the loss or alteration of information (Saull et al., 2001). Even unintentional events
that damage information systems may cause important information to be lost or corrupted.

In the ever-changing technological environment, security within organisations has to keep up-to-date with such changes. Organisations must put safeguards in place to protect their information. This is done to minimize the impact if and when security measures are breached and vulnerabilities are exploited.

Information security has added the need for trust and accountability in electronic transactions, such that for most organisations, the security objective is met when (Saull et al., 2001):

- Information is available and usable when required (*availability*);
- Information is observed by or disclosed to only those who have the right to know (*confidentiality*);
- Information is protected against unauthorised modification (*integrity*);
- Business transactions and information exchanges between enterprise locations or with partners can be trusted (*authenticity and non-repudiation*).

Nowadays, a great deal of business information remains far from transparent due to technology. Company information that is on an employee’s PC can be manipulated and unintentional mistakes can occur. Unethical behaviour towards business information by employees can damage a business. Information security helps in preventing data corruption, unauthorised damage or alteration of business information (Sophos\(^b\), 2004). However, information security is often treated solely as a technology issue, when it should also be treated as a governance issue (Business Software Alliance, 2005). Engagement from management is commonly penned as governance.
1.3 Corporate, IT and Information Security Governance

1.3.1 Corporate Governance

Corporate governance is about promoting corporate fairness, transparency, and accountability (Stralser, 2004 & Hinson, 2005). It is a very important function that aids an organisation in safeguarding shareholders’ interests. In other words, corporate governance’s primary concern is business performance, understood in a competitive and financial sense (Bloem et al, 2006).

The core aspects of corporate governance include (Hinson, 2005):

- Appropriate management structures;
- Management control frameworks with clear accountability and responsibility;
- Ethics in the business context and social responsibilities;
- Risk management – risks in general, including operational, financial, market and IT risks;
- Management oversight and independent review – making sure that managers and staff comply with internal and external rules, regulations and laws (compliance and audit functions);
- Transparency, i.e., open and honest communication by management to stakeholders about the true state and future aspects of the organisation.

Corporate governance is different from other types of governance (such as financial or IT governance), and it is regarded as the principal form of governance for organisations (Bloem et al., 2006). Ultimately, corporate governance involves the return of money to those who invest in and own the corporation.
1.3.2 IT Governance

IT governance focuses on the business value of IT within an organisation. As Koen Brand and Harry Booen (2004) explained, IT governance is an integral part of business operations and an integral ingredient of corporate governance. However, many organisations still associate IT governance with compliance requirements rather than a framework that can be used to enhance the value of IT in their organisations (PricewaterHouseCoopers, 2007). IT governance should be designed to ensure that IT adds value to the business and that IT risks are mitigated.

The growing dependence of most companies on their information systems, together with the risks and benefits IT carries with it, have made IT governance an increasingly critical component of overall governance (Saull et al, 2005). Furthermore, as security for information becomes a central concern across industry and government, it is essential that good governance exist to ensure proper protection and integrating information security with corporate governance (Conner et al, 2004).

1.3.3 Information Security Governance

Information security is concerned with the “protection of valuable company assets and processes” (Gillespie et al, 2004). Governance, in turn, concerns itself with the way in which an “organisation is being managed” (Verine⁸, 2004). When the two are put together, information security governance is formed.

Information Security Governance (ISG) is a subset of corporate governance dealing with the policies and internal controls related to information resources and their security (Entrust, 2005). ISG is a topic of immediate concern for all
companies that use electronic communication media such as the Internet (Verinea, 2004), because as soon as a company is connected, it is vulnerable to attacks and threats. ISG is concerned with how management and executives will consider and administer information security within their organisations as they may incur personal liability for failed information security (Verinea, 2004). This is due to the introduction of legislation in this regard.

1.4 The Legislative Response

1.4.1 Terminology Defined

This research uses terminology that needs to be explained in order to explicitly clarify its meaning in the context of this research (Wikipedia, 2007):

- **Law** is a system of rules that people are supposed to follow in a society or a country. The courts and police enforce this system of rules and punish people who break the laws, such as by making them pay a fine or other penalty or sending them to jail. In ancient societies, laws were written by leaders, to set out rules on how people can live, work and do business with each other. Today in most countries, laws are written and voted on by groups of elected politicians in a legislature, such as a parliament or congress. To follow the laws of a society is to do **legal** things. An activity is **illegal** if it breaks a law or does not follow the laws.

- **Regulations** are legal restrictions enforced (and clarified) by government through the creation of regulations.

- **A treaty** is an agreement under international law affecting organisations dealing internationally.

- **Accords** are similar to agreements between parties.
For the purpose of this research, the term “legal source” refers to the collection of the previously mentioned terms (law, regulation, treaty and accord).

1.4.2 Legal Sources

Enron and WorldCom were not the only organisations that went bankrupt due to unethical behaviour by their executives. Other organisations were Arthur Andersen, Tyco, Adelphia and many more (Stralser, 2004 & Loyd, 2004). Notably, similar ethical risks are present in today’s corporate world. In addition to eliminating these risks, legislation has been implemented to regulate corporate fraud, violations of privacy and identity theft that occurs in today’s organisations (Sophos, 2004). These laws control organisations that fail to express the characteristics of good corporate governance, such as Enron and WorldCom. Emerging guidelines, legislation and standards were created to increase awareness and understanding of all the risks that organisations may encounter (Olson et al, 2005). This assists in the creation of a secure infrastructure that protects sensitive customer information. The regulations also govern the way that businesses conduct their affairs (Cohasset Associates, 2005).

The Enron and WorldCom scandals reinforced the need for widespread governance improvements (Hinson, 2005), and the passing of new regulations to govern the organisations. Additionally, after the September 11, 2001 terrorist attack, regulators moved quickly to enact legislation aimed at strengthening information security and fraud detection (Citrix System, 2004).

Regulations such as the Sarbanes-Oxley Act (SOX) were created in response to the management and high-profile accounting scandals of organisations such as Enron (Information Builders, 2004). This regulation was created to hold corporate executives personally responsible for the accuracy and consistency of information
stored or located anywhere in the organisation (Smith, n.d. & Information Builders, 2004). Executive management must provide an effective assessment of the security controls that safeguard organisational information (Smith, n.d.).

The Sarbanes-Oxley Act is viewed as a turning point in the governance of organisations, especially with regard to the direct involvement of management (Bloem et al., 2006). The challenge for managements is that they will face criminal penalties if they fail to meet regulatory requirements (Sophosb, 2004 & Pasley, 2005). Thus, an organisation’s confidence will be restored because the directors’ signatures will appear on clear business decisions that are based on accurate data (Bloem et al., 2006).

An example of a regulation that is applicable to the banking industry is the Basel Accord. Financial markets were always prone to heavy losses resulting from poor risk management policies or fraud (Nayak, 2004). Regulations such as the international Basel Capital Accord (Basel II) have been designed to harmonise the international banking regulations by demanding proof of robust compliance controls and forcing management to be involved in the compliance activities (Information Builders, 2004). The Basel II was designed to align capital-adequacy requirements more closely with the risks that are found in the banking industry; therefore, it can be used to aid risk-management and risk-measurement capabilities within the financial industry (Mboweni, 2004).

Regulations are a first step in addressing problems, such as fraud and violation of privacy, which arise when organisations abuse the way they manage information (Sophosb, 2004). However, to achieve compliance, organisations first must align their operations to the regulatory rules and other requirements associated with the business (Cohasset Associates, 2005). It is recognized that to achieve this
presents a seemingly insurmountable challenge, as is subsequently discussed in the problem statement of this research.

1.5 Problem Statement

As businesses expand more and more into the cyber-world, so too does the need to secure the information they have (Mallela, n.d.). Information used by companies needs to be protected as it is very critical to a business’s 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, n.d.) and, from a legal perspective, to avoid businesses being sued by internal or external parties.

It is recognized that managements have realized the importance of information security and understand their responsibilities towards corporate governance (Narayanan, 2004). Corporations are also aware that there are guidelines that can be used to identify security controls in order to protect their informational assets. Guidelines, standards, legislations, regulations and best practices, such as the Control Objectives for Information and related Technology (COBIT), the Basel Accord, the Sarbanes-Oxley Act, the Banks Act, the Electronic Communications and Transactions Act (ECT Act) and others, can be used to this effect, and additionally, help companies to understand the rights and responsibilities of board members and business and IT managers.

However, the problem is that companies today face a barrage of IT and security compliance requirements. Sarbanes-Oxley and the security and privacy regulations that preceded it force companies to adhere to a complex and often
overlapping series of controls that impact on almost every part of their organisation (Getronics, 2005). There are various guidelines and standards that make it almost impossible for management to know which guideline and standards to use or leave out (Mitchell, n.d.). To complicate matters, the language of all the acts is vague (Sophos\textsuperscript{a}, 2004). For example, the Sarbanes-Oxley Act holds officers of the company responsible for establishing “internal controls” without defining them. Furthermore, organisations are under a surge of “compliance helper” products. These tools do not offer the kind of solutions required to address broad security issues across a company (Sophos\textsuperscript{b}, 2004). An organisation cannot view compliance with each law (e.g. SOX) in isolation.

Therefore, the problem being investigated in this research comprises the confusion caused by the proliferation of legislation, regulations, standards and guidelines which companies must comply to. With so many regulatory demands being placed on businesses, it is easy for an organisation to use guidelines that are irrelevant to their line of business (IT Week, 2005). It is also easy for the compliance programmes to become a huge drain on organisational resources, with each programme focusing on its own objectives and possibly even working against the objectives of other programmes.

\section*{1.6 Limitations in Scope}

In terms of the scope of this research, the afore-mentioned problem scenario will be investigated within the ambit of the South African financial sector. The South African banking sector is also affected by a growing list of regulations, because some of the largest banks have expanded internationally (Winterboer et al., 2002). Therefore, it is important for South African banks to comply with international as well as local laws, regulations and guidelines that affect them.
These will be identified in Chapter 3, as this research cannot consider all the relevant legislation, regulations and guidelines.

A further limitation on the scope of the research relates to the content of the regulations and legislations that will be investigated. For the purpose of this research, the focus is only on the security and privacy issues that are relevant in protecting financial information in South African financial institutions.

It must be emphasized that the analysis of legal sources conducted in this dissertation is not meant to be authoritative. It is intended only to serve the purpose of concept demonstration. Legal advice must be taken from qualified, specialist legal advisers because the author of this dissertation is not a legal expert.

1.7 Objectives of the Study

The primary objective of this research is to propose a compliance model that enables financial institutions to comply with the laws and regulations that influence the South African financial sector. The proposed compliance model addresses the following:

- The privacy and protection of financial information that is stored, processed or passed by a South African financial institution;
- Simplification of the effort that is required in order to comply;
- Elimination of redundancy found in various legislations and regulations.

In order to reach the primary objective of the research, the following secondary objectives are also addressed:

- The importance of securing financial information that is used in the financial sector;
• An investigation of the legal sources that influence financial institutions in securing the information that is stored, processed or passed by them, in particular, in the South African sector;
• Finding a way to consolidate the requirements of various legal sources that influence the South African financial sector;
• The provision of an information security model for regulatory compliance from the perspective of the South African financial sector.

1.8 Methodology

The research conducted for this project is primarily of a phenomenological nature. This is also known as interpretivist research - the researcher gathers information and filters it, while involving him/herself in the study. In this kind of research, subjectivity plays a role, with the researcher having to argue towards his/her interpretation of the research area and the proposed solution.

Firstly, the researcher conducts a literature study covering the following areas:
• The financial industry’s awareness of security issues that impact on financial information;
• The importance of securing financial information for financial institutions that have expanded their businesses into the cyber-world;
• The regulations that governs the South African financial industry and aid in securing financial information;
• The importance of having a compliance model to consolidate regulatory requirements for securing financial information.

After the literature study, the researcher, through logical argumentation, proposes an integrated compliance model, the South African Banking Sector
Legal Compliance Model (SABS-LeCoM). Lastly, the model is applied, using a fictitious scenario, to serve as a proof-of-concept.
1.9 Layout of the Dissertation

Chapter 1 gives a brief background to the study in order to highlight the problem at hand, the objective of the research, and the methodology used to achieve the objective. Chapter 2 examines the financial industry’s awareness of security issues and the impact technology has on securing information, as well as the controls that can be used to mitigate the vulnerability of assets (such as financial information). Moreover, it also discusses the current status of the South African financial industry.

Chapter 3 focuses on certain regulations that can be used in the identification of security controls that aid in mitigating the risk of threats, and give a brief overview on the need for them. Additionally, issues that relate to regulations and business’ competitiveness, such as the relationship between IT and different regulations, are also pointed out. Furthermore, regulations that affect the South African financial sector are discussed. The identified regulations are outlined, as well as their impacts on IT, and the compliance issues as regards each regulation are explained. Moreover, it looks at the ways IT and regulations can be used together to protect financial information.

Chapter 4 explains the proposed compliance model (SABS-LeCoM) in detail, and the benefits of the model are also illustrated. Chapter 5 considers the SABS-LeCoM and applies it as a proof of concept. The chapter focuses on how the SABS-LeCoM can be implemented within South African financial services. Chapter 6 concludes by summarizing the reason for the dissertation and how the objectives of the research were reached and the limitations of the research. Furthermore, it also gives a brief overview on the proposed model for the financial sector. The layout of the chapters is illustrated diagrammatically in Figure 1.1.
Figure 1.1: The chapter breakdown structure of the dissertation

Chapter 1
Introduction

Chapter 2
South African Financial Institutions and Financial Information Security

Chapter 3
Legal Sources

Chapter 4
A Model for Legal Compliance in the South African Financial Sector

Chapter 5
SABS-LeCoM - Proof of Concept Using Privacy and Internal Controls

Chapter 6
Conclusion
1.10 Conclusion

This chapter showed that information is regarded as the most important asset of an organisation, and it is imperative that it is protected. However, technology has brought along with it unethical behaviours from some organisations as they try to see what they can get away with. Therefore, this chapter suggested that companies must do their best to adhere to ethical standards, which are top-down efforts from leadership (Stralser, 2004). Good ethics and governance can lead to success in business.

The next chapter will continue to focus on the security of information, in particular financial information. Additionally, the South African financial industry and the industry’s shift to the cyber-world will be addressed. Security issues that relate to the cyber-world will also be discussed, as well as the controls that can be used to mitigate the risks triggered by these security issues.
Chapter 2
South African Financial Institutions and Financial Information Security

"It is impossible to make anything foolproof because fools are so ingenious"...
Murphy’s Law

2.1 Introduction

The information age has brought along with it significant advances, challenges and changes, thus resulting in businesses becoming more complex (Verine, 2004). These advances include using the cyber-world as a market place with the aid of new technology, as has been implemented by various South African banks. This issue is further explored in Section 2.3. However, Kevin Beaver (2003) states that although these changes enhance financial services for customers and assist employees while lowering the overall IT costs for the financial industry, security vulnerabilities are increased.

This chapter gives a brief background to South Africa’s financial industry and what it entails. Moreover, it addresses the financial industry’s shift to the cyber-world. The cyber-world has benefits but also limitations, especially for industries that need to expand their businesses into different marketplaces.

After discussing the financial sector’s shift to the cyber-world, security within this sector is outlined. Mechanisms that can be used in the protection of financial information are also discussed. This leads to a discussion on internal controls to illustrate the importance of securing information, and in this case, financial
information. The financial industry deals with information daily and it is of utmost 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). Furthermore, there are guidelines to help businesses with the protection of information through the selection and implementation of security controls. The loss of, or unauthorized access to, information will result in a financial loss to an institution. Therefore, proactive steps must be taken in protecting financial information because internal and external attacks are constantly searching for vulnerabilities (Olson et al, 2005) within the organisational systems or any other system available.

The discussion on internal controls is the final point of discussion in this chapter, thereby setting the scene for a discussion of legal sources that can be used to identify security controls in Chapter 3. Financial institutions are obliged by the government to protect financial information. Emerging legal sources, such as guidelines, legislation, regulations and standards, have been created to increase the awareness and understanding of all the risks that organisations may encounter (Olson et al, 2005). This assists with the creation of a secure infrastructure that protects sensitive customer information. In order to understand why security is so important in the financial industry, this chapter firstly starts with an overview of the South African financial industry and then explicates some issues which are key to the increased importance of security.
2.2 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). Because there are different types of businesses and sectors, the industry is a complex one. The financial industry is made up of three primary types of service categories, namely (Macdonald, 1998 & Ramarapu et al, 1996):

- Banking;
- Mutual funding companies;
- Insurance and other financial institutions.

Notably, South African financial institutions that offer banking services are obliged to comply with the Banks Act, before any other law, regulation, guideline or standard, in order to be recognised as banks. This dissertation will focus on South African banks, rather than other financial institutions that do not primarily offer banking services. It is recognized though that banks do not only offer banking services, but overlap with services primarily classified in the mutual funding and insurance categories (and vice versa). The dissertation will nevertheless refer to financial institutions or the financial services sector, with the understanding that the mutual funding and insurance categories were not investigated in depth. A brief overview of each of the banking, mutual funding and insurance service categories is subsequently provided.

2.2.1 Banking

According to Singh (2004), the South African banking sector can be traced back to the Mother City (Cape Town) and was influenced by British and Dutch banking
traditions. Nowadays, the South African global banking sector consists of the ‘big four’ namely: Standard Bank Group, First National Bank Group, Absa Group and Nedcor (Mboweni, 2004 & Singh, 2004). The market share of these banks is shown in Figure 2.1.

![Figure 2.1: 2002 Market Share of the “Big Four” South African Banks (Singh, 2004)](image)

The “big four” dominate the South African banking sector (Marais et al, 2004 & Mboweni, 2004), and offer different types of services. The typical services provided by banks include (Stichele, 2004 & Singh, 2004):

- savings;
- cheque accounts;
- transmission accounts;
- notice deposits;
- fixed deposits;
- long-term finance;
- credit cards;
- short-term insurance;
- medium-term investments;
• merchant banking;
• small business banking; and now also
• Internet banking.

Banks help stabilise a country’s finances, and help it to grow economically and socially (Wiese, 2004). Without stability and growth, the country’s upliftment of living standards would be almost impossible (Wiese, 2004). Banks have little choice but to create large organisations that have the power to deploy the resources needed to fight competition from both existing banks and powerful newcomers (Marais et al, 2004).

2.2.2 Mutual Funding

A mutual fund provides a way for people with common financial goals to group resources together (Oppenheimerfunds, 2006). Whether people are planning for their personal retirement, education savings, business retirement plan, or any other needs, mutual funds are designed to match personal situations (State Farm, 2006) and offer a variety of investment choices to influence their situation. Factors that can influence people’s investment choices include (State Farm, 2006):

• Personal financial goals;
• How soon they need the money;
• How much they can comfortably afford to invest;
• And the preferred investment style.
2.2.3 Insurance Services

According to Stichele (2004), insurance is a promise of compensation for a potential future, unexpected loss, in exchange for a periodic payment. Insurance services are designed to enable consultants and industry and regulatory organisations to evaluate and better manage risks and exploit business opportunities in the global insurance market (Business Monitor Online, 2005).

Insurance can be sold either to individuals or companies through insurance agents (Stichele, 2004). Forms of individual insurance include (Business Monitor, 2005 & Stichele, 2004):

- Health insurance
  - Specifies the type of medical treatment for the insured person;
- Life insurance
  - Guarantees payment to the beneficiaries when the insured person dies;
- Personal property insurance
  - Such as vehicles and homes that an insured person owns;
  - Specifies which property, accidents, theft and other damages are covered.

Insurance services to organisations include (Business Monitor, 2004):

- Liability: e.g., of board members, environmental damage;
- Damage of organisational property: e.g., computers, goods;
- Fraud and other financial problems;
- Transport;
- Extra payment to employees: e.g., for long-term illness, accidents, unfair dismissal, etc.
Among the issues (such as the AIDS epidemic) facing South African insurers, there are moves to enhance public confidence in the industry through transparency and disclosure, together with consumer education (Stichele, 2004). The insurance service continues to grow, and according to the figures provided by the Business Monitor (2005), will continue to grow beyond 2005 (Glaessner et al, 2002).

Following this brief overview of the primary categories of services in the financial industry, the focus now shifts to the financial industry’s transition to the cyber-world, and the issues that arise from this noteworthy transition.

### 2.3 The Financial Industry and the Shift to Cyber-World

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 has also got caught up in the hype of moving to the cyber-world because there is no physical product that needs to be delivered (Singh, 2004), and its customers can be easily swayed to use the Internet services (Dombi, 2001). Furthermore, customers will not be standing in long queues to effect transactions, which will result in pleased customers (Singh, 2004).

Nevertheless, customers find it more comforting if they know that their bank has an actual physical building that they can go to - even if it is just one (Dombi, 2001). They would rather know that there is also a physical place where they can still go and perform transactions, rather than only doing them online. According to Moody (2002), online banking is the fastest growing service that banks can offer in order to gain and retain new customers. Customers are able to access
their accounts online and make transactions without the problems of going to a physical bank. However, as stated by Dombi (2001), the physical bank also needs to be there so that the customers can feel secure knowing that they can get help from it as well.

The business benefits from the shift to the cyber-world can be to generate additional revenue, improve customer services, extend marketing, and increase cost savings (Gow, 1997). Many authors agree that the Internet market is on the increase. Jeff Levick (eMarketer, 2004), Head of Financial Services Vertical Group Google said that, "The Internet will continue to extend the reach of regional and national financial institutions, enabling banks of all sizes, and in all areas, to compete for customers, nationally and even internationally, with a wide range of services." The implications are that the Internet will continue to flourish and be one of the most competitive markets where ease of use, customer services and customer satisfaction take priority (Dombi, 2001).

The shift to the cyber-world comes with benefits but also technical problems. These problems include (Stichele, 2004):

- Safety and security in e-finance on the Internet;
- Coordinating different software between divisions;
- Coordinating the technological integration after a merger or acquisition.

In line with the focus area of this research, the main issue that will be discussed in the upcoming section is security concerns pertaining to financial information. The importance of protecting financial information and the current state of security in the financial industry will also be discussed.
2.4 Financial Information and Security

The financial industry is using technology to change the way business is done, from the creation, distribution, storage and sharing of information (Binary Consulting, 2005). South Africa is, in many ways, a global leader in the adoption and use of technology to improve competitiveness and delivery in the financial services industry (BMI TechKnowledge group, 2005). However, technology also creates security vulnerabilities and opens avenues for threat agents to explore. Therefore, the importance of security in an increasing technology-centric world cannot be underestimated.

2.4.1 Importance of Security

According to Deloitte (2004), the concept of security has expanded from merely protecting assets and people to sustaining business, no matter what types of disturbance might occur. These disturbances can range from computer viruses to acts of terrorism. The main focus is to make sure that assets are protected from threats (Maphakela et al, 2005). The top IT risks that a financial institution can encounter are theft of identity data or fraud (Eject, 2004), which can lead to unauthorized access and transfers.

South African financial institutions are regarded as well-developed and sophisticated, with an infrastructure and an emerging market status in the economy to match (Winterboer et al, 2002). Furthermore, the big four retail banks in South Africa are using the Internet as a business opportunity to improve on their competitiveness and delivery. However, the Internet has created security breaches in South African financial institutions by exposing vulnerable information to those who can infiltrate them (Rose, 2000).
Lombard (2003) in “Expert Proves that Latest Measures Don't Protect Online Customers”, discusses one of the best-known financial service security breaches in South Africa. Absa’s customer information was retrieved via a program that was sent to Absa’s Internet customers. Lombard (2003) explains that the program installed itself on Absa customers’ machines and tracked the customers’ keystrokes, capturing all their necessary details and sending the information back to the hacker. He further disputes the measures (online password keypads and firewalls) that Absa implemented to overcome this problem. After the Absa breach, the other banks also upgraded their security systems in order to avoid being attacked (Lombard, 2003). They also introduced safety precautions on their sites, so that their clients could read them and be aware of security threats and how to protect themselves (Eject, 2004).

Financial institutions are more vulnerable to financial threats because of their roles as monetary depository institutions, and also because they handle confidential customer information (Gillespie et al, 2004); therefore, this information needs to be protected from all of these threats that are increasingly becoming stronger and more dangerous. One of Symantec’s reports on Internet security revealed that financial services firms experienced the highest number of malicious virus attacks during a certain period in 2003 compared to other industries (Gillespie et al, 2004). Except for malicious virus attacks, there are also other threats that can really affect organisational business processes. These threats, classified as internal and external threats by Gillespie et al (2004), are subsequently discussed.

### 2.4.2 Threats that Affect Organisations

The financial industry deals with information daily, and it is of outmost importance that this information is protected, as has been mentioned before.
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).

External threats are becoming more and more complex. The types of external threats that most financial institutions and other businesses are concerned with are (Gillespie et al, 2004):

- Phishing:
  - This scam is when a customer receives an email from a third party masquerading as his/her financial institution. Then the criminals use the information gathered to access the customer’s account to steal his/her money;
- Customer impersonation:
  - The name explains itself. Customer impersonation is an attempt by criminals to gain secret information or change it online. A related scam is when the criminal takes the name of a deceased person and uses it to file loan applications, which are then sent to a broker in another city;
- Application security weakness:
  - A weakness that can be exploited when the attacker gains full access to the system and data;
- Hardware theft:
  - Security of physical assets is often neglected or overlooked even though it is very critical in protecting the financial information residing on the hardware.

Additionally, there are also internal threats that must not be overlooked (Gillespie et al, 2004). “Internal threats” do not refer to bad guys, gangsters or even
hackers as many would think (Bruck, 2002). The types of internal threats that companies should be aware of include (Bruck, 2002 & Gillespie et al, 2004):

- **Employees**
  - An employee with access to sensitive data, such as account numbers;
  - Employees or former employees that know the weaknesses of the software being used and have the ability to introduce viruses into the system;

- **Viruses**
  - Viruses coming from opening an e-mail. Viruses can also be regarded as external threats as they are from outside the organisation;

- **Fraud**
  - This is likely to be theft of identity data, which can lead to unauthorised payments and transfers.

According a survey done by Ernst & Young (2004), it was found that one in five employees reported personal awareness of other individuals stealing from a computer. Fraud was found to be one of the top ten risks for organisations (Ernst & Young, 2004), with viruses and employees’ misconduct topping the table (see Figure 2.2).
A financial institution can be damaged in many ways because of fraud. In 2003, 56% of all identity theft fraud was bank-related (Gillespie et al, 2004). The resultant brand erosion can make the institution lose its customers and a decrease in online transactions can be seen (Gillespie, 2004). Therefore, there is a need for security in the financial industry and the ways of protecting financial information must keep ahead of possible threats.

### 2.4.3 Security in the Financial Industry

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

Companies that lose control over customer information face enormous losses financially, such as lawsuits from customers, costs of responding to incidents and loss of revenue from some customers that stop doing business with them (Cenzic, 2005). Therefore, financial information needs to be secured and some form of control needs to be in place to ensure that security risks are minimised and controlled. Corporations are aware of these requirements, and are also aware that there are legal sources that can be used to identify security controls, in order to protect the informational assets (Maphakela et al, 2005). These legal sources help financial institutions to assess vulnerabilities against threats, to identify internal controls and to introduce mechanisms, policies and procedures that can be used to mitigate the risks.

Legal sources also introduce various countermeasures, such as information security programmes, that can be used to secure information. Nowadays, financial services have undertaken radical security measures to help protect customers' sensitive financial information with the usage of legal sources (Dombi, 2001). Regulations provide a good index of what processes and controls are expected in an information security programme (Moore, 2003).

The information security programme of a financial institution is, arguably, the most important aspect of maintaining an appropriate security posture, because its aim is to decrease the number of information security incidents and reduce risk occurrence (Kairab, 2004 & Moore, 2003). Many topics addressed by an information security programme to improve security include: risk assessment, encryption, physical security, business continuity, logical access controls, and any
other security control or process that mitigates threats to customer information (Moore, 2003 & Kairab, 2004). Numerous companies have introduced some form of information security programme into their organisations in order to mitigate security risks.

Security can be improved in many ways, and Dekker (1997) suggests that a robust defence requires a flexible strategy that allows adaptation to the changing environment. This can be done by introducing policies, procedures and technology to support the implementation and the changes that occur over time (Dekker, 1997).

In the context of this research, the important thing is that businesses must use legal sources to identify internal controls that can be used to protect important financial information. Legal sources help in identifying internal controls that need to be strengthened in order to comply with different legal sources (McGuire, 2005). The focus, therefore, is what information security measures financial institutions are required to implement, as required by law. Chapter 3 will focus more on the legal sources that affect the financial industry and discuss these in more detail, whereas the focus of the next paragraph is to explicate internal controls, their selection and use to protect informational assets.
2.5 Internal Controls

An internal control is a process which provides reasonable assurance to management and other personnel about the achievements of objectives in the following categories (BMI, 2005):

- Effectiveness and efficiency of operations;
- Reliability of financial reporting;
- Compliance with applicable laws and regulations.

Some people see internal controls as the end itself, but internal controls should be viewed as a means to the end. They should be seen as an opportunity for people to work together in order to achieve the same goal, which is to provide reasonable assurance of information security.

Internal controls include not only financial matters, but also operational and compliance controls, and management of business risk associated with a company (King Report, 2002). They are also based on established policies and procedures and are implemented by trained, skilled personnel, whose duties have been appropriately separated from other employees.

A survey done by Rittenberg and Miller (2005) showed that most of the participants believed that their companies had gained valuable awareness throughout all levels of their organisations about internal controls and the need for them. Most survey participants wrote comments supporting their view that management and employees more fully understand how controls affect operations and that management accepts responsibility for controls.

Internal control helps an organisation achieve its objectives of securing financial information. Although internal controls do not ensure success, they require
everyone’s responsibility in order to achieve their objectives. Additionally, internal controls have a greater influence in reducing operational risks and managing these operational risks.

### 2.5.1 Operational Risk Management and Internal Controls

Operational risk in financial institutions has been defined as the risk of loss from breakdowns associated with the conformation, netting, settlement and accounting of financial transactions (Kos, n.d. & Tortoriello, 2004). This class of risks has an unlimited downside and can expose an institution to serious financial and reputational losses, as evidenced in recent, well-publicised, large corporate failures around the world. Examples of these were discussed in Chapter 1 (Sections 1.1.1 – 1.1.3).

Financial services such as banks are exposed to various types of operational risk, including the potential losses arising from internal activities or external events caused by breakdowns in information, communication, physical safeguards, business continuity, supervision and procedures and agency responsibilities (African Development Bank Group, 2005).

Managing operational risk is not new, especially for financial institutions (Crawford et al, 2005). Financial institutions have been aware for many years, of the hazards and uncertainties arising from IT infrastructure, fraud, human resources and many similar issues (Crawford et al, 2005). In an organisation, even the most anonymous person in the office can “sink the ship” (Milligan, 2004). The essential truth about operational risk is that everyone has some control over it. Andrew Wilson suggests that good people should be employed, and having a good culture can have an effect of minimizing the operational risks (Milligan, 2004). The number of business failures is on the increase, and this
renews the visibility of risks under the banner of “operational risk” (Crawford et al, 2005).

2.5.2 Groups of Controls

Some papers refer to these as types of controls and others as classes of controls, and for this dissertation, the ‘groups of controls’ reference will be used. There are three groups of controls (Brewer et al, 2004) that can be used to ensure that informational assets are secured from threats. They are:

- Preventive Controls
  - A control designed to avoid unintended events or results (Contrast with detective controls) (COSO, 1992);

- Detective Controls
  - A control designed to discover an unintended event or result (Contrast with preventive controls) (COSO, 1992);

- Corrective Controls
  - Designed to correct errors or irregularities that have been detected (COSO, 1992).

An effective internal control helps an organisation achieve its operational, financial reporting and compliance objectives with the aid of internal control components. Internal controls consist of five components that are interrelated to each other (RGB & Co., 2005). These components must be present to help an organisation understand the effectiveness of the internal controls in place. These components are identified, using the US framework called the Committee of Sponsoring Organisations (COSO, 1992). The components will not be discussed in detail as they require an in-depth look at each component, which would detract
from the focus of this research. An overall summary of each of the components is given below (COSO, 1992 & HP, 2003).

- **Control Environment**: The foundation for all other components of internal control, providing discipline and structure. The control environment sets the tone for the entire organisation.
- **Risk Assessment**: The entity’s identification and analysis of relevant risks, forming a basis for determining how to manage them.
- **Control Activities**: The policies and procedures that help to ensure management’s directives are carried out.
- **Information and Communication**: Processes and systems that support the identification, capture and exchange of information in a form that enables employees to carry out their duties.
- **Monitoring**: Processes that assess the quality of internal control performance over time.

Management’s role in the internal control system is critical to its effectiveness (Country of Orange, 2003). Management should not look at every piece of information, like auditors have to, to determine the effectiveness of the controls in place. They should focus their monitoring activities in high-risk areas and leave the other parts to auditors.

### 2.5.3 Selecting the Right Controls

Managements have realized the importance of information security and understand their responsibilities towards corporate governance (Williams, 2003 & Ernst & Young, 2004). In selecting the right controls, organisations must develop a defensible case for reasonable and appropriate controls that address practically anticipated risks (MetaGroup, 2005). An organisation will identify its security
requirements in order to select the correct controls (ISO 17799 SOUTH AFRICAN STANDARD, 2000). According to the ISO 17799 (2000), there are three main sources that can be used to identify security requirements:

- Risk Assessment
  - Assessing threats to assets, vulnerabilities to and likelihood of occurrence and potential impact are established;
- Legal, statutory and regulatory requirements
  - Regulations that different services have to satisfy or comply with;
- Principles, objectives and requirements for information processing
  - Those that organisations have developed to support their organisational specific operations.

Once security requirements have been identified, controls should be selected and implemented to ensure that the security risk is mitigated to an acceptable level. However, the document (ISO 17799) consists of controls that are not applicable to every information system for an organisation; therefore, an organisation will have to identify the correct controls that affect it (ISO 17799, 2000). A good ongoing risk assessment is also very important and can help determine what controls need to be put in place (Moore, 2003).

This dissertation will focus on the second source of identifying security controls, that is, the legal, statutory and regulatory requirements. Information on legal sources for a specific sector (the South African financial sector) will be discussed in the forthcoming chapter (Chapter 3).

**2.6 Conclusion**

This chapter gave a brief background of the South African financial industry and what it entails. Furthermore, the importance of securing financial information
against threats was discussed. Financial information is regarded as an extremely important asset and needs to be protected from threats. Threats such as viruses, worms and fraud are increasingly becoming more hazardous and powerful. Therefore, it can be concluded that it is significantly important that customer information held by financial institutions be protected and kept confidential. To this end, the chapter provided an overview of internal controls as an aid in protecting financial information. Although internal controls per se do not ensure information security success, they nevertheless help financial institutions to accomplish the objectives of securing financial information, reducing operational risks and managing residual operational risks. As discussed in this chapter, management’s involvement in the process of securing information is key for the success and effectiveness of internal controls.

The next chapter will continue focusing on securing financial information and more specifically, using legal sources as a way to help mitigate information security risk. Furthermore, the chapter will discuss the influences legal sources have on technology and ways to improve security of information with the aid of technology. Additionally, the chapter will outline legal sources that affect the South African financial sector as well as the impact they have on it.
Chapter 3

Legal Sources

"For where morality failed, the law now has to rush in to fill the void." - Thabo Mbeki.

3.1 Introduction

While Chapter 2 discussed the importance of securing financial information, this chapter will look at different legal sources that can be used to protect this vital asset. Also in Chapter 2, different types of threats that can affect an organisation were mentioned. Threats such as phishing, customer impersonation, fraud and others need to be mitigated. There are controls that can be used to secure the processes that businesses need in order to succeed (Refer to Chapter 2 – Section 2.5 Internal Controls). Additionally, there are various legal sources that can be used to identify the security controls that can help in mitigating the risk of threats. Legal sources that will be identified for protection of financial information within the context of this dissertation include legislation, regulations, accords and reports.

This chapter will focus on these legal sources, and give a brief overview on the need for them. Additionally, issues that relate to legal sources and business’ competitiveness, such as the relationship between IT and different legal sources, will also be pointed out. Furthermore, the legislation, accords and reports that affect the South African financial sector will be discussed. The identified legal sources will be outlined, as well as their impacts on IT, and the compliance issues as regards each of these legal sources will be explained. Moreover, it will look at
the ways IT and the identified legal sources can be used together to protect financial information.

### 3.2 The Need for Legal Sources within Organisations

Many legal sources (e.g. legislation, regulations, etc.) are forcing companies to change the way they manage their information (Sophos, 2004). With the greater shift from paper-based to electronic documents, organisations are required to secure their electronic documents as well (Captaris, 2005). Organisations that have a huge amount of data, such as financial institutions and healthcare organisations, are required to manage and safeguard their electronic records from threats (*Threats are discussed in Chapter 2*).

Electronic records can include any information about a business customer held by a business. It is information that is stored in an electronic format, and it needs to be protected from anyone who is not authorized to access it. These electronic documents are now being used in court as evidence to support cases. However, the electronic records may be used as evidence only if it is established that they are accurate (Fish & Wildlife Service, 1995). Therefore, it is necessary for organisations to secure and maintain these documents (Captaris, 2005).

The accuracy of electronic records implies that they need to be documented in order to recover the correct information (or records) when needed. Some organisations have taken an interest in data archiving in order to recover the correct information in time (Aimes, 2005). They are also taking a far more active interest in digital rights management in order to ensure the integrity of data archives (Aimes, 2005). Digital rights management is a form of archiving and it will not be discussed further in this chapter.
Legal sources, such as the King Report (2002), require organisations to archive their electronic records for a minimum period of time so that they can be retrieved when needed in court (Aimes, 2005). Many organisations are realising the need for legal sources to guide them in securing information, so that they can protect themselves when required (Silverberg, 1999). Financial services are heavily regulated with regard to their record retention requirements because of laws that affect them (Captaris, 2005 & RSA Security, 2005). The laws that are affecting the financial sector will be discussed in the coming sections.

There is a greater need for regulation in the financial services sector because financial services carry a huge amount of society’s cost and consumers need to feel confident of the service (Falkena et al, 2001 & Financial Service Technology, n.d.). Furthermore, legal sources are a first step in addressing problems which arise when organisations disregard the importance of their information (Sophos, 2004); moreover, if anything happens, like a huge disruption, it is easier to keep businesses running (Tumpell-Gugerell, 2005). The company will continue running through the guidance of legal sources used to secure its information.

**For example:**
9/11 shocked the world and made everyone realise that even the world powers, such as the US, are not invincible, and anyone is vulnerable (The Teen Center, 2001). Also, during that time, billions of euros were injected into Europe alone, a few hours after the events in New York. This was done to secure the financial information and capitals of consumers. Thus, one key focus of regulation is on safety, namely to ensure the containment of systemic risk (Tumpell-Gugerell, 2005).
The crucial objectives of regulation should be to achieve a high degree of economic efficiency and consumer protection in the economy (Falkena et al, 2001). However, at a more practical level, the objectives are threefold, namely to sustain (Falkena et al, 2001):

- Systemic stability;
- The safety and soundness of financial institutions;
- Consumer protection.

The main focus of this dissertation is on the third objective, namely ‘consumer protection’ in financial institutions, which, in a sense, is supported by the achievement of the first two objectives, viz systemic stability and the safety and soundness of financial institutions. In particular, the focus is on the use of financial service legal sources in protecting consumer information.

Emerging legal sources have been created to increase an understanding of all the risks that organisations may encounter (Olson et al, 2005). Legal sources assist with the creation of a secure infrastructure that protects sensitive customer information. Some legal sources provide guidance for information privacy and security to help maintain public trust and protect their assets in financial institutions (RSA Security, 2005). Trust between a consumer and an organisation can soon be eroded by people who disregard the importance of privacy, when there is no regulation to protect either of them (Symposium, 2003).

Regulation is not only about managing the way the financial market operates. It is also about deterring and preventing financial crime. Of course, there can be no doubt that this is desirable, but even this aspect of regulation can have a downside (Financial Service Technology, n.d.). For example, when it comes to ensuring that IT systems in one organisation are integrated with those of another, legal requirements can hamper this process quite severely. Needless to say, such
complexities grow exponentially when these organisations are located in different countries with different legal systems and requirements. However, what kind of impact do legal sources have on the IT operations of businesses? There is a need to know the impact because most businesses depend totally on their technology-based systems to run their daily operations (Williams, 2003).
3.3 Legal Sources – The Impact on IT Operations in Financial Services

Rapid improvements in technology in the past decades have had dramatic consequences on financial services, such as the protection of customer information (White, 2001). As discussed in Chapter 2, information security is vital for the success of a business. Additionally in Chapter 2, the necessity to identify security controls to protect the confidentiality, integrity and availability of information was stated.

These days, IT has an influential part in the running of businesses because most processes are driven by IT systems (Williams, 2003). Moreover, it has been noted that most of a business’s functions use computers. It is almost difficult to imagine a successful organisation without a certain level of IT influence (IT Governance Institute, 2004).

The financial service was one of the first sectors to embrace the process of IT governance (Williams, 2003). In financial institutions, IT plays a major role in aiding business processes because financial reporting processes are driven by IT (IT Governance Institute, 2004). This role played by IT grows as technology advances and more threats and risks are created for financial institutions (Ramsaran, 2003).

Advances in technology have given financial services the capability of performing more tasks over different geographical areas to reach new markets. Financial services’ Internet exposure has brought along with it online banking and more services (Barnes, 2004). Barnes (2004) raises issues that consumers are aware of that are inherent to the use of the Internet as a banking tool. These include the protection and the usage of customers’ non-public personal data. ‘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 (Maphakela et al, 2005). Financial managers are concerned with the maintenance of customer information in order to retain and attract customers because it is critical to their institution’s success (Ramarapu, 1996 & Illet, 2005). Also, financial services must rise to security challenges, or they risk losing their customers (Illet, 2005). Therefore, financial institutions have used information technology as a means to secure information. The question to be asked is how is IT used in the South African financial industry to secure this information?

IT should assist South African financial institutions with obtaining resources needed to manage compliance issues from an IT perspective (Ramsaran, 2003) and help lessen the risks. IT also helps financial institutions in assessing their financial reporting processes in order to comply with regulations, legislation, reports, accords and other legal sources. The problem that most South African financial institutions, or any other businesses face, is the compliance costs of these legal sources.

Compliance costs are costs that are incurred in complying with legal sources (Pearson Education, n.d.). Compliance costs and process improvements can quickly absorb a large percentage of profits within smaller institutions (SoftwareTest, 2005). Therefore, for some institutions, it is difficult and also expensive to increase both the compliance and technology budget (TowerGroup, 2005). On the other hand, larger institutions with resources are able to influence management with regard to IT spending to improve compliance efficiency (SoftwareTest, 2005).

IT has a massive accountability requirement that did not exist more than ten years ago, in terms of governance (Bruno-Britz, 2005). IT governance ensures
that IT contributes effectively to enhance the organisation’s shareholder value (Williams, 2003) and is enforced through various legal sources. For example, as noted in Chapter 1 (Section 1.4), the SOX Act is considered a seminal development in the governance of organisations, which holds management personally liable for failure to meet requirements specified in legal sources. It is much easier for CIOs to prove compliance and to control their IT infrastructure if they adhere to standards and frameworks that aid in complying with SOX (Ensom, 2005). Jim Ensom (2005) further states that from an IT perspective, SOX requires management to use a recognized risk control framework to evaluate overall compliance. Examples of such frameworks include the Control Objectives for Information and related Technology (COBIT) and the ITIL Framework for IT Service Management, which can be used to improve the effectiveness and efficiency of business operations and support financial reporting (Kahn, 2004 & Ensom, 2005). These frameworks help to provide a basis for addressing many of the IT-related governance issues.

The expansion of the South African financial service into the global market has had benefits to the country’s economic growth (Mboweni, 2000). South African financial services have used technology in order to enter the global market and achieve financial growth. However, as said before, there are many risks which accompany the benefits associated with the use of technology. For the financial services industry, risk has always been an inherent part of doing business (SAS OPRISK Management, 2005). The use of new and emerging technologies, however, brings a whole new dimension to the meaning of risk. Legal sources are needed to regulate the use of technology and the protection of consumer information, also in the South African financial sector.
3.4 Legal Sources Affecting the South African Financial Sector

The South African banking sector is affected by increasing regulatory compliance requirements because some of the largest banks have expanded internationally, as was already mentioned in Chapter 2 (Winterboer et al., 2002). Therefore, it is important for these leading banks to comply with international legal sources that affect them, while at the same time complying with local legal sources. For the purpose of this dissertation, the focus is only on the security and privacy issues that are relevant in protecting financial information for South African financial institutions.

Various aspects of the legal instruments applicable in the South African financial sector will now be examined. The focus will be on both local and international legal sources, although it must be stated upfront that due to scope limitations, the investigated list of legal sources is not necessarily exhaustive and focuses on sources that are considered prominent and are well discussed in the relevant literature.

3.4.1 Local (South African) Legal Sources

Four primary local sources of legal instruments that make provision for security and privacy of information and apply to the financial industry were identified, namely:

- The King Report on Corporate Governance for South Africa (King II Report, 2002). The dissertation uses the King Report as a basis for compliance because it promotes high standards for governance in the context of South African companies.
• The Financial Intelligence Centre Act (FICA) suggests that reasonable measures must 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).

• The Electronic Communication Transaction Act (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 financial institutions that transact electronically.

• 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).

Each of the afore-mentioned laws as well as the King Report is subsequently discussed in more detail.

3.4.1.1 The King Report

The King Committee on Corporate Governance launched the King Report on Corporate Governance for South Africa in 2002 (King II Report, 2002) at an Institute of Directors Conference. The King Report applies to all companies listed on the board of the JSE, such as large public entities, banks and other financial and insurance entities (King Report, 2002). The purpose of the King Report is to promote the highest standard of corporate governance for companies.
3.4.1.2 The Financial Intelligence Centre Act

The Financial Intelligence Centre Act (FICA) states 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 an effective money-laundering control system that will decrease the problems of authentication issues (Hofmeyr, 2006).

The Act requires the identification and verification of clients or people involved in the transaction conducted in order to minimise the risk of the institution being abused by criminals (FICA - Section 21(1), 2003). The Act also 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, n.d.). The FICA’s primary role is to provide high-quality financial intelligence about criminal activities to help law enforcers. Furthermore, it places an obligation on any person filing the report to document suspicious or unusual transactions (FICA – Section 29, 2003 & Hofmeyr, 2006). This can lead to identifying the individual involved in malicious or criminal activities, thus helping both law enforcers and IT to develop security controls that reduce the risks stated in the report.

3.4.1.3 The Electronic Communications and Transactions Act (ECT Act)

The South African ECT Act was established with a view to (ECT, 2002):
• providing for the facilitation and regulation of electronic communications and transactions;
• providing for the development of a national e-strategy for the Republic;
• promoting universal access to electronic communications and transactions and the use of electronic transactions by SMMEs;
• providing for human resource development in electronic transactions;
• preventing abuse of information systems;
• encouraging the use of e-government services; and
• providing for matters connected therewith.

It is, therefore, clear that the ECT Act has an impact on financial institutions that transact electronically, as mentioned previously. The ECT Act also focuses on the privacy of information in one of its chapters (Chapter VIII of the ECT, 2002). The 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.

3.4.1.4 The Banks Act

For an institution to lawfully carry on the business of a bank, it needs to use the Banks Act as a baseline for all the banking service requirements (Banks Act, 1990). This means all the banks have to follow the Banks Act in order to be regarded as banks, and be allowed to perform banking functions. A bank’s functions in the financial services industry include 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).
This concludes the overview of local or South African legal sources that either primarily or secondarily address the protection of financial information. The focus now shifts to similar sources, but from an international viewpoint, given that Banks that transact internationally would need to comply with those also.
3.4.2 International Legal Sources

Three international legal sources that are widely known and discussed were identified. These include:

- The Gramm-Leach-Bliley Financial Services Modernization Act (GLBA). This financial legislation defines financial structures and how to protect financial information (Broaddus, 2000). The GLBA is investigated in this dissertation because it is widely used, and it affects South African financial institutions with international operations.

- The Sarbanes-Oxley Act (SOX) is a law that requires firms to certify the integrity of their financial records, their information disclosure controls and internal controls (Business Software Alliance, 2005). The SOX Act is United States-oriented, and it was selected as it applies to global companies trading in the US.

- The BASEL Accord (Basel II) is a treaty aimed at improving the security and soundness of a financial system (Wilson, 2002). All of the major banks that have international operations are governed by compliance with the Basel II in countries where it was either incorporated by reference into local law or assented to by the state. Basel II is the second of the Basel Accords, which are recommendations on banking laws and regulations issued by the Basel Committee on Banking Supervision. Since it has to be incorporated into local laws in order to be applicable, it can, in a sense, be considered as an international standard.

The following section will give an overview and some of background of the Gramm-Leach-Bliley Act (GLBA) and the compliance issues that can be expected
from it. Moreover, the sections from the GLBA that are relevant in the protection of financial information will also be discussed.

### 3.4.2.1. The Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act 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, n.d.). According to the Federal Trade Commission (n.d.), the Gramm-Leach-Bliley Act (GLBA) protects consumers’ personal information held by financial institutions.

This law is US-oriented and is called Gramm-Leach-Bliley (GLBA) as it was named after chairmen of the congressional committee primarily responsible for its development, namely Senator Gramm, Congressman Leach and Congressman Bliley (Broaddus, 2000). The GLB Act requires companies to give consumers privacy notices that explain the institutions’ reasons for sharing the consumers’ information (Federal Trade Commission, 2005). The GLBA allows consumers the right to limit some – but not all – sharing of their information with other institutions (Federal Trade Commission, 2005).

Broaddus (2000) discusses the three main focuses of the GLBA in his dissertation. Firstly, he states that it establishes what the structure of the financial industry will be for the foreseeable future. Secondly, the GLBA establishes how this new structure will be regulated and supervised. And thirdly, it establishes new requirements with respect to community reinvestment and the right of customers to protect the privacy of their personal financial information. The main focus of
the GLBA is to protect customers’ personal information and addresses affiliation amongst financial industries (Moore, 2003).

As discussed so far, the GLBA is a legislation that covers the privacy of consumer information-sharing between institutions and the rights the consumers have to their information. The next sub-section will cover the section that influences the protection of consumer information in terms of the collection, privacy and the sharing of financial information.

**The Gramm-Leach-Bliley Act and the Protection of Consumer Information**

The GLBA is not a set of instructions to be followed to ensure compliance; federal financial agencies are delegated the duty of compliance (Moore, 2003). It is a legislation that defines the financial structure, and how to protect financial information (Broaddus, 2000). The GLBA consists of seven titles and various sections that address the relationship between financial institutions, insurance, privacy and other financial industry legal sources (Cenzic, 2005 & Moore, 2003). However, as mentioned in the Chapter 1, Section 1.6, this research has limitations to the content of the legal sources. Therefore, for the GLBA, the focus here is on a section that deals with the protection of non-public personal information, called Section 501 – Protection of Non-Public Personal Information (Barnes, 2004). To recap, as noted in Section 3.3, ‘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 (Maphakela et al, 2005).

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

Section 501 of the GLBA, therefore, forces financial institutions to (Vormetric, 2004):

- ensure the security and confidentiality of customer information;
- protect customer information from threats;
- protect customer information against unauthorized access or usage.

The next section will give an overview of the Sarbanes-Oxley Act (SOX) and will give an explanation of Section 404 of the SOX, which was selected for further discussion in this dissertation. Section 404 was identified and investigated as it aids in the protection of consumers’ financial information. Additionally, the impact of SOX on IT will also be examined.

### 3.4.2.2 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 US-oriented, but it does apply to global companies trading in the US such as South African banks trading in America. This dissertation will focus on one section of the SOX, namely Section
404, which deals with the internal controls that are relevant for financial institutions’ compliance regarding financial information security (Gordan, 2005).

As mentioned previously, the SOX Act is an American legislation that covers broad topics that businesses must consider to ensure compliance (Sophos, 2004). Sarbanes-Oxley is a name that is extracted from two legislators, Senator Paul Sarbanes and Representative Michael Oxley (Williams, 2005). The SOX requires both public and commercial companies to comply with it.

The SOX Act requires public companies to certify to the integrity of their financial records, their information disclosure controls and internal controls (Business Software Alliance, n.d. & eProject, 2004). This law 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 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 were introduced and discussed in Chapter 2.

Failure to comply with SOX can result in the CEO (Chief Executive Officer) of the business getting into trouble with the law (Williams, 2005). The excuse from a CEO of “not having any idea of what is going on under him/her” is no longer accepted (SOX Community Forum, 2004). Therefore, management needs to take full acceptance of its organisation’s responsibilities, as most legal sources affect the entire organisation and not only a specific department. SOX affects the entire organisation, as shown in Table 3.1 below. Notably, finance and IT departments are greatly affected by this law.
<table>
<thead>
<tr>
<th>Departments Impacted on by SOX</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance</td>
<td>100%</td>
</tr>
<tr>
<td>IT</td>
<td>95.7%</td>
</tr>
<tr>
<td>Sales</td>
<td>43.5%</td>
</tr>
<tr>
<td>Human Resources</td>
<td>39.1%</td>
</tr>
<tr>
<td>Customer Service</td>
<td>30.4%</td>
</tr>
<tr>
<td>Marketing</td>
<td>17.4%</td>
</tr>
<tr>
<td>Other</td>
<td>8.7%</td>
</tr>
</tbody>
</table>

Table 3.1: Departments Affected by SOX (Braunstien, 2005. & Exler, 2003)

It is extremely important for executives to recognise that the SOX Act affects IT, as IT plays a major role in most companies’ information and records (Braunstein, 2005). Most IT executives take complying with SOX very seriously because they have realised that their jobs are at stake (Exler, 2005). However, in Paul Williams’ article (2003), Peter Morriss is quoted as saying, "The IT aspect of corporate governance is one of the things that chief executives (CEOs) think they don't have to understand - until it affects their organisation."

The next sub-section will cover Section 404 of SOX that influences the protection of consumer information in terms of the collection and the distribution of financial information.

**SOX and the Protection of Consumer Information**

SOX is organised into 11 titles, and consists of sections that deal with the collection and the distribution of financial information (SOX404, 2004 & SOX Community Forum, 2004). The following topics are covered by the 11 titles of the SOX Act (Braunstien, 2005):

- Reporting – improving disclosure requirements;
Roles – strengthening corporate governance;
Conduct – expanding on accountability;
Enforcement – improving oversight;
Penalties – broadening sanctions;
Relationships – forcing auditor independence.

As mentioned previously, this dissertation will focus on Section 404 of the SOX Act as it is likely to have the greatest long-term impact on IT’s compliance role (Kahn, 2004).

According to the IT Governance Institute (2004), Section 404 affects corporate management, executives and financial officers and requires the management of public companies to report annually on their companies’ internal controls over financial reporting (McGladrey & Pullen, 2005). It is important to understand what ‘internal controls over financial reporting’ actually means. This is defined by Sophos (2004) as the responsibility of the company’s management to provide reasonable assurance regarding the prevention or timely detection of unauthorised attainment, use or disposition of the assets that could have a serious impact on the financial statements. For example, if an organisation can identify that its main asset is information and the main threat is constituted by computer viruses, then it is up to management to make sure that the necessary controls are put in place to protect that information. In this case, anti-viruses would be put in place to minimise the impact of an attack. But that is not enough security as new viruses are identified daily, weekly, or even hourly. Therefore, it is up to management to make sure that the anti-virus software is effective enough to protect the information or assets from new or old viruses, for example, through the attainment of regular updates to virus signatures.
Section 404 also requires proof of the effectiveness of a company’s internal controls with the aid of the company’s auditor to attest to, and report on, management’s assessment of internal controls (McGladrey & Pullen, 2005). Therefore, management is required to provide a report that states whether the internal controls are effective or not (IT Governance Institute, 2004). The auditor will verify that management’s assessment is correct and controls are implemented correctly. Section 404 consists of an internal control report that contains statements of (RBG & Co, 2005 & IT Governance Institute, 2004):

• Managements’ responsibilities for maintaining/establishing adequate internal control structures and procedures for financial reporting;
• A statement identifying the framework used by management to evaluate these controls (e.g. COSO);
• Management’s assessment of the effectiveness of internal controls;
• And a statement that an independent auditor has issued an opinion on management's assertion.

Furthermore, management need to enclose any changed internal controls or added controls to minimize the vulnerabilities that were identified since the previous or last internal control report.

The last legal source identified from an international viewpoint is the Basil Capital Accord.

3.4.2.3 The Basel Capital Accord (Basel II)

The new Basel Capital Accord (Basel II) is an improvement on the 1988 Capital Accord (Basel I) that focused on the capital the banks have, and the costs if the banks fail (Wilson, 2002). The main focus of the Basel II is on the internal controls and management of financial systems (Wilson, 2002). Furthermore, both
Basel I and Basel II attempt 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).

Basel II focuses on internationally operating banks, and its principles are also designed to be applicable to banks of different scales of complexity. Many financial services believe that Basel II will likely to lead to improved capital allocation and more efficient processes (McDowall, 2005). Andy Efstathiou (2002) believes that the Basel II will:

- Aggressively increase the amount of outsourcing in the financial services industry;
- Decrease the value of infrastructure services and increase the value of business process services to this vertical;
- Cause banks to outsource for competitive advantage, rather than to drive cost savings;
- Drive upgrades to reporting and monitoring tools for the financial industry;
- Focus services vendors away from disaster recovery and toward business continuity;
- Aggressively increase the amount of consolidation in the financial services industry.

As South Africa becomes a global player, South African businesses have to comply with international legal sources, such as the Basel Capital Accord (SARB, 2005).
There is a lot of demand from government for institutions to prove that they have robust control measures to protect consumer information. Basel II will help South African financial institutions improve (SARB, 2005):

- corporate governance and risk management;
- capital management and stronger capital structure;
- transparency standards;
- supervisory practices and processes.

### 3.5 Conclusion

Financial institutions are in the business of taking risks for their customers and are, as a result, subject to a high level of supervision and control (Information Builders, 2004). It is of utmost importance that the information held by a financial institution is secured. In this chapter, the legal sources that can assist in identifying security controls were identified and discussed. From the overview presented in this chapter, it is clear that financial services are heavily regulated by the various laws that affect them. The problem is that there are various legal sources such as legislation, reports, and accords that make it almost impossible for management to know which legal source to use or not (Mitchell, n.d.). This constitutes the crux of this research, namely to find a solution to the proliferation in legal sources that South African financial institutions must comply with. To this effect, Chapter 4 will propose a legal compliance model for South African financial institutions.
Chapter 4
A Model for Legal Compliance in the South African Banking Sector

4.1 Introduction

Whereas Chapter 3 focused on the importance of legal sources, this chapter proposes a legal compliance model for the South African banking sector. Chapter 3 furthermore identified various legal sources that have an impact on the South African financial industry, both locally and internationally. Legal sources such as the King Report, Basel Accord, ECT Act, and the FICA, just to name a few, were identified and discussed in Chapter 3 (Refer to Chapter 3 – Section 3.4 Legal sources affecting the South African Financial Sector).

The sheer volume and complexity of legal sources reduce their effectiveness (Hassel et al, 2001 & Calder, 2006), as they are difficult to understand and to know which parts to use or leave out (IDC, 2005). Therefore, a strategic perspective, such as a compliance model, can help in simplifying the compliance effort required to comply with legal sources (Getronics, 2005). Furthermore, having a common architecture can enable solutions to be mapped to a specific regulatory requirement (Brabeion, 2006). In Section 4.2, the reasons for needing a compliance model will be expanded. Additionally, the chapter presents and explains the proposed legal compliance model in detail from Section 4.3. The benefits of the model will also be illustrated.
4.2 Why a Compliance Model?

An increasing number of legal sources are imposed on companies, including South African banks. A recent survey of attendees at a CSO Interchange event, held in June of 2005 in Chicago, found that 74% of attendees believed that their organizations must comply with more than five regulations and not surprisingly, 64% of respondents said that they were more concerned about compliance in the current year than the previous year (CSO, 2005), thereby implying increasing awareness and pressure from a legal point of view.

As new laws emerge on a regular basis, many businesses are finding it difficult to keep abreast with new compliance requirements from legal sources (Calder, 2006). Market surveys suggest that because many companies face the need to comply with multiple regulations, their security teams are overworked trying to keep up with compliance-related tasks, so much so that security team members are often pulled off of their other important security duties (Getronics, 2005). The requirements of most legal sources 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. It follows that there is a definite need for a compliance model to ameliorate the situation.

A compliance model can aid organisations with low-cost compliance, competitive advantage in addressing compliance challenges, reduced costs and the distribution of compliance initiatives, amongst others (Calder, 2006). A compliance model promotes a hierarchical approach to compliance improvement (Australian Government, 2005). A hierarchical approach is used because it will
allow a top-to-bottom approach in identifying the necessary legal requirements and breaking them down into simpler and usable parts. The idea of this approach is to maintain the principle of identifying a regulatory element, and being able to recognise the legal sources that cover that particular element (Treaster, 2005).

An *element*, in the context of this research, is a legal requirement to comply with as stated in a particular law. An *element* from one legal source will be compared with *elements* from other legal sources in order to identify whether they are similar or not. It therefore constitutes the unit of comparison for the purpose of discovering redundancies across the various legal sources.

Having considered and shown the need for a legal compliance model, the model that is proposed is subsequently discussed.
4.3 Proposed Compliance Model and Benefits

In this section the South African Banking Sector Legal Compliance Model (SABS-LeCoM) is proposed to solve the problems discussed in Section 4.2. The model is based on five principles, viz.:

1. Facilitation of a top-down approach to legal compliance to ensure the inclusion of all applicable legal sources;
2. Getting rid of unnecessary overlapping requirements in the various legal sources;
3. Establishing the legal sources that include a particular legal element;
4. Enabling solutions to be mapped to specific legal elements contained in various (known) legal sources; and
5. Promoting a unified approach towards legal compliance which dovetails with other security initiatives.

The SABS-LeCoM consists of four phases. The phases (as illustrated in Figure 4.1) are:

1. Legal source identification;
2. Identification of sections relevant to the issue of concern (e.g. security and privacy);
3. Assessment of sections (to identify common and unique elements);
Figure 4.1: SABS-LeCoM – A High-Level Diagrammatic Representation
The benefits derived from the application of such a compliance model, include:

- Compliance management for multiple legal sources rather than individual laws;
- Optimization of resources – less time, money and people are required to implement and maintain a unified compliance approach;
- Elimination of redundancies found in various legal sources;
- Reduction in overall compliance monitoring efforts; and
- Combination of efforts and resources towards security initiatives, with legal compliance efforts.

The coming section will discuss the four phases of the SABS-LeCoM in detail.
4.4 The Phases of the SABS-LeCoM

4.4.1 Phase 1: Legal Source Identification

This phase will clearly define the required legal sources to support the compliance initiative and is the first step forward. Since the model is targeted at the South African financial services sector, the legal sources that affect this sector must be identified. This will be illustrated in the proof-of-concept chapter (Chapter 5). As stated previously, there are various legal sources and not all legal sources affect
all types of institutions. Resources will be allocated by the organisation to identify the legal sources that affect it. The result of this process is a list of the relevant legal sources.
4.4.2 Phase 2: Identification of Sections Relevant to the Issue of Concern

Moving to the second phase of the model, the next requirement is the identification of sections included in the legal sources that are relevant to the issue of concern, which in this case pertains to the security and privacy of information. Each individual legal source must be reviewed to identify the relevant sections. It is conceivable in both this phase and in phase 3, that financial organizations do not have to work in isolation and reinvent the wheel. There are various sources addressing legal compliance management which would assist companies in this regard, for example Getronics (2007) and Unified Compliance Approach (Adler, 2006), amongst others.
4.4.3 Phase 3: Assessment of Sections

Figure 4.4: Element identification through the Investigation process

The third phase of the model comprises a continuous process which requires an intense assessment of the sections identified in Phase 2. This phase deals with the process of identifying elements which are common and those which are unique to each of the legal sources. It is constituted as follows:

1. **Step 3.1 Review and List Elements**
   List all the elements from the sections of all the legal sources that deal with the issue of concern.

2. **Step 3.2 Identify and Allocate Categories**
   Arrange the identified elements into categories that relate to what is being achieved. The categorisation can be determined according to the common requirement the elements are trying to achieve.
3. Step 3.3 Compare Elements

Execute a comparative analysis of the elements to check whether they contain overlapping requirements.

For the purpose of clarification, Steps 3.1 – 3.3 can further be explicated as follows:

- Elements from one regulation that deal with the issue of concern are listed;
- An element from a next regulation is compared to each one of the elements already on the list;
- As elements are compared to each other, categories are identified to place the element within the issue of concern;
- An element that is not similar to ones on the list, but which focuses on the issue of concern, is added to the list;
- Elements that contain overlapping requirements with elements already included on the list, are cross-referenced against the elements that are already on the list (i.e. a new element will only be added if it has new requirements, but a record (cross-reference) will be kept of all the legal sources referring to the same elements);

The final list of elements and cross-references can be compiled either into a document or preferably a database to facilitate future reference and maintenance.

This explication is subsequently depicted in Figure 4.5, starting with the identification of the relevant legal sources through to the classification of the elements. The diagram is explained as follows:

- Three legal sources are identified (Legal source 1, Legal source 2, Legal source 3);
The elements from each legal source that focus on the protection of information are identified (Elements x, w, a, j);
Finally, similar and unique elements are grouped accordingly (Categories k and m).

Figure 4.5: Assessment of legal sources, sections and elements

The execution of this phase results in the identification of common elements that have been combined together and distinctively arranged to avoid redundancy. Non-similar (or unique) elements are also identified and arranged and categorized as well.
4.4.4 Phase 4: Implementation of Solutions

Lastly, Phase 4 of the model deals with the implementation of solutions to comply with the legal requirements of the common and unique elements identified during Phase 3. This phase requires diligent mapping of the requirements (elements) to solutions while ensuring that the selected or envisaged solution(s) satisfies the requirements of all the legal sources.

Of importance during the execution of this phase, is to ensure that the fifth principle on which the SABS-LeCoM is based, is satisfied. The principle, as listed in Section 4.3, stated that an approach that ‘promotes a unified approach to legal compliance and which dovetails with other security initiatives’, is followed. This implies that the solutions that are implemented in this phase, can also serve towards other security initiatives. For example, if the institution is rolling out the ISO 17799 “Code of Practice for Information Security Management”, then the controls recommended by this standard, could serve as controls (or solutions) for the legal compliance effort. This means that the list of elements compiled from
the legal sources and cross-referencing the various legal instruments that include the elements (see Step 3.3), should include a list of controls or solutions, which again cross-reference other security initiatives where these controls are of relevance.

This approach minimizes the complexity of complying with multiple legal sources, and provides a single view of regulatory compliance, as supported by Sundararajan et al. (2006) and further integrates with other institutional security initiatives.
4.5 Conclusion

The output of this research is a model that provides a roadmap for concomitant conformance with legal sources in the financial sector. This model was proposed because of the need to follow a unified compliance approach, rather than having multiple randomized compliance projects, each focused on an individual law. In this chapter, the SABS-LeCoM, the need for such a model and the advantages that can be gained from it, were discussed. A diagrammatic representation of the model was explained at the level of the four phases which constitute the model.

The model has been designed to eliminate the redundancy of the same elements that can often be identified in different regulations. It further minimizes the complexity of complying with multiple legal sources and provides a single view of and approach to legal compliance.

The next chapter will focus on providing a case study of legal sources affecting the South African banking sector as a proof of concept, in order to illustrate the usage of SABS-LeCoM by South African banks.
Chapter 5
SABS-LeCoM: Proof of Concept Using Privacy and Internal Controls

5.1 Introduction

Based on the introduction of the South African Banking Sector Legal Compliance Model (SABS-LeCoM) in Chapter 4, this chapter presents a proof of concept of the model through investigation of a number of legal sources affecting South African banks. For the purpose of the proof of concept, a number of elements from the identified legal sources were selected as it would be unmanageable to within the scope of this research project, do a comprehensive analysis of all legal sources.

This chapter uses a scenario (provided below) to show how the SABS-LeCoM can be used within the financial service environment. The scenario will give a brief background of a fictional South African financial institution and the problems the institution has encountered. A fold-out diagram of the SABS-LeCoM is included at the end of this chapter for easy reference while reading this chapter (Figure 5.1).

Scenario

A typical South African financial service company – Bank X – holds sensitive information that has been collected to provide services to its customers, such as information about customer savings and loans, short term insurance, home loan insurance, etc. Bank X has also invested in establishing an infrastructure for internet banking, to serve its local customer base but also to support
requirements from an international perspective, as it has recently expanded its business abroad.

Given the sensitive nature of the information held by Bank X, it is understandable that the bank has been targeted by threat agents and has faced attacks where privileged information was lost. The bank has suffered loss of faith from the public and its customers due to these attacks being reported in the press. It further had to reimburse the losses of its customers in lieu of the intense public scrutiny that followed these events.

In order to address the situation, the bank has implemented some security controls to minimise the impact of security breaches, such as basic safeguards like anti-virus solutions, anti-spyware and authentication and access control systems. These attempts have, however, not stopped the security breaches from occurring.

Bank X knows that the information it has collected is very important and needs to be secured, as it is sensitive. The bank also realises it must show that due care was taken to protect the information it keeps, as this is required from a legal perspective. BUT, how will Bank X comply with the privacy- and security-related requirements posed by legal sources relevant to institutions operating as financial service companies in South Africa?
5.2 SABS-LeCoM – Proof of Concept

The previous chapter (Chapter 4, Sections 4.3 and 4.4) explained and discussed the four phases of the SABS-LeCoM, which to reiterate, are:

1. Legal source identification;
2. Identification of sections relevant to the issue of concern;
3. Assessment of sections (to identify common and unique elements);

Assuming that Bank X is applying the SABS-LeCoM to bring itself in line with the demands of relevant legal instruments, the afore-mentioned phases must be executed. Each of these phases is subsequently discussed, as pertaining to Bank X.

5.2.1 Phase 1: Legal Source Identification

The first phase of the model requires that all legal sources that are relevant to the compliance effort be identified. Therefore, Bank X will allocate resources within the organisation to execute the first phase of the model, to identify all legal sources that affect them as a South African financial institution. Relevant international legal sources must be identified as well because Bank X operates internationally and therefore they are affected by these legal sources. The result of this process is contained in Table 5.1.
5.2.2 Phase 2: Identification of Sections Relevant to the Issue of Concern

During phase 2, an analysis of the legal sources is required to determine which parts (or sections) are applicable to the issue of concern. In this case, the issue of concern (for Bank X) is to protect and secure financial information they have acquired over a number of years. Therefore Bank X will apply this second phase to identify sections, within identified legal sources, which affect the security and privacy of their financial information. Both the local and international legal sources listed in Table 5.1 will be reviewed.

Table 5.2 lists the identified legal sources and the sections that affect the issue of concern relevant to Bank X.
<table>
<thead>
<tr>
<th>LEGAL SOURCE NAME</th>
<th>SECTION OR PART APPLICABLE TO SECURING INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>King Report</td>
<td>Section 2 - Risk Management</td>
</tr>
<tr>
<td>Basel Accord</td>
<td>Part 4: The Third Pillar – Market Discipline</td>
</tr>
<tr>
<td>Gramm-Leach-Bliley Act</td>
<td>Section 501</td>
</tr>
<tr>
<td>Sarbanes-Oxley Act</td>
<td>Section 404</td>
</tr>
<tr>
<td>Financial Intelligence Center Act</td>
<td>All the Sections</td>
</tr>
<tr>
<td>Banks Act</td>
<td>All the Sections</td>
</tr>
<tr>
<td>ECT Act</td>
<td>Chapter VIII</td>
</tr>
</tbody>
</table>

Table 5.2: Legal sources and the sections that focus on securing information
5.2.3 Phase 3: Assessment of Sections

Phase 3 of the SABS-LeCoM requires an in-depth analysis of the sections of the legal sources that are relevant to securing information. Bank X will therefore move on to Phase 3 of the model in order to assess the sections identified during Phase 2. Elements that are common between the legal sources and those which are unique to each of the legal sources, will be identified. In order to achieve this, the three steps of Phase 3 are executed, viz:

- Step 3.1: Review sections and list legal elements
- Step 3.2: Identify categories
- Step 3.3: Compare elements

Each of these steps is subsequently discussed in the context of Bank X and the legal sources and sections listed in Table 5.2.

5.2.3.1 Step 3.1: Review Elements

Bank X will list all the elements from each section of a legal source that deals with the securing of information. The following sub-sections provide a list of the elements relevant to the issue of protecting information for each identified legal source. Recall from Chapter 4, Section 4.2, the definition of a legal element as being a legal requirement to comply with as stated in a particular law.
5.2.3.1.1 The King Report

The King Report (2002) recommends that the controls effected by a company should encompass the following:

- The information systems environment;
- Reliability and integrity of financial and operating information;
- Effectiveness and efficiency of operations;
- Safeguarding of assets;
- 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.
5.2.3.1.2 The Electronic Communications and Transactions Act

As mentioned in Chapter 3, 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 (ECTA, 2002). The list below mentions some of the criteria needed to implement and comply with the ECT Act.

- Information must be disclosed in writing to specify the purpose for which any personal information is being requested, collected, collated, processed or stored.
- Information held by third party may not be disclosed unless required by law or authorized to do so in writing by the consumer.
- Information should be disclosed in a secure manner.
5.2.3.1.3 The Financial Intelligence Centre Act

The Financial Intelligence Centre Act (FICA) states that financial institutions cannot execute a transaction with a client that has not been identified (Manuel, 2004). The list below mentions some of the criteria needed to implement and comply with the FICA.

- Identification of clients and other persons, the verification of information and the maintaining of records.
- May not establish a business relationship or conclude a single transaction with a (new) client unless the prescribed steps have been taken to obtain the information relating to the client.
- Where the client represents someone else, the keeping of records of the identity of the person so represented and also the authority of client to represent such other person;
- Records of the relationship or transaction between clients must be maintained, such as names; documents; identity of client, etc.
- Facts and circumstances of a suspicious or unusual transaction must be immediately reported to the relevant people involved.
5.2.3.1.4 The Banks Act

As discussed in the previous chapter, the Banks Act is used as a basis for banking services. It is used as a basis because it stipulates the requirements for the lawful carrying on of the business of a bank (Banks Act, 1990). The pointers below amend the Banks Act of 1990 (Banks Acts, 2002).

- To regulate the conducting of a due diligence audit of the financial condition of a bank
- To prohibit the appointment of an employee of a bank as chairperson of the audit committee of that bank or the appointment of the chairperson of the board of directors of a bank as a member of the audit committee of that bank.
- To introduce further safeguards in respect of large exposures constituting credit risks to banks and to apply such safeguards also to controlling companies, local branches of foreign banking institutions and foreign branches of local banks.
- To extend the Registrar of Banks' discretion to exempt a bank from the prohibition on the pledging or encumbering of its liquid assets.
- To make further provision regarding the use of a name by a bank or by a foreign institution that conducts the business of a bank by means of a branch in the Republic;
- To do away with the process of judicial management of a bank that is in financial difficulties and, instead, to regulate the process of curatorship of such a bank more comprehensively.
5.2.3.1.5 The Sarbanes-Oxley Act

The list below shows some of the requirements for compliance with the SOX (Breisacher, 2004) that are stated in Section 404 of this Act.

- Data must be retrievable after long term-retention, even as new technologies are introduced.
- The 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.
5.2.3.1.6 The Gramm-Leach-Bliley Act


- Ensure confidentiality of information.
- Prevent unauthorised access (authentication or access).
- Protect customer data against anticipated hazards or threats.
- Protect customer data integrity.
- A financial institution 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.
- The privacy notice must include accurate statements of a company’s privacy practices.
- The 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.
• The board or committee of the board must receive annual reports on the status of the information security programme.

• Consumers and customers have the right to “say no” to having their information shared with certain third parties.

• Customer information must be disposed in a secure manner.

• Wherever possible, minimize the amount of personal data given to commercial or governmental entities.

• Review the bank’s risk management processes for implementing effective measures to protect customer information.

• There must be regular testing on the effectiveness of controls, systems, and procedures of the information security program.
5.2.3.1.7 The Basel Accord

The South African financial industry is highly committed in making sure that it is compliant with Basel II by 2007 (SARB, 2005). The list below mentions some of the criteria needed to implement and comply with it. The main focus is on the operational risk management requirements.

- There must be an independent operational risk management function that is responsible for the design and implementation of the bank’s operational risk management framework.
- Audit of user activity
- Audit of allocation of the user rights
- The output must be an integral part of the process of monitoring and controlling the bank’s operational risk profile.
- There must be regular reporting of operational risk exposure and loss experience to top management.
- The operational risk management system must be well documented.
- Internal and/or external auditors must perform regular reviews of the operational risk management processes and measurement systems.
5.2.3.2 Step 3.2: Identify and allocate Categories

After reviewing and listing elements that are relevant to the securing of information, Bank X will further consider each element for the purpose of categorising it. To reiterate, in Chapter 4 it was stated that the categorisation must be determined according to the common requirement the elements are trying to achieve. For the purpose of this dissertation, the following are the identified categories that best describe the goal of the legal elements:

- Privacy and protection issues;
- Internal controls;
- And elements that fall outside of this categorisation, but are nevertheless relevant to comply with the legal requirements.

Each of the legal elements must therefore be allocated one of the categories listed above.

5.2.3.3 Step 3.3: Compare Elements

Following the identification and allocation of categories to each legal element, Bank X will now compare the elements with each other to check whether they are already being handled by another element from another legal sources or not. In other words, the process is executed as follows:

- Elements from one legal source that deal with the privacy and security of financial information are listed;
- Elements from another legal source that also deal with the privacy and protection category, are compared to each one of the elements on the list;
Each element that is not included on the existing list, but which focuses on the issue of concern, is added to the list;

Elements that overlap with elements already included on the list, are cross-referenced against the elements that are already on the list (i.e. a new element will only be added if it has new requirements, but a record (cross-reference) will be kept of all the legal sources referring to the same elements);

The process is repeated until all the legal sources have been investigated.

The following table (Table 5.3: Common issues found in legal sources that affect Bank-X) shows a summary of requirements for the identified sections of the legal sources that affect Bank-X.

<table>
<thead>
<tr>
<th>Privacy and Protection</th>
<th>Identification, reviews and assurance reporting of internal controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Safeguarding of assets</td>
<td>1. A statement of management’s responsibility is needed for establishing and maintaining adequate internal control over financial reporting.</td>
</tr>
<tr>
<td>Assurance on the effectiveness and efficiency of operations within the organization</td>
<td>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.</td>
</tr>
<tr>
<td>2. A financial institute must provide an initial privacy notice to customers not later than the time the relationship commences.</td>
<td>3. Rehearsals and reviews on a regular basis are necessary to ensure that plans are</td>
</tr>
<tr>
<td>3. Location where the media is stored must be highly</td>
<td></td>
</tr>
</tbody>
</table>
Privacy and Protection | Identification, reviews and assurance reporting of internal controls
---|---
controlled.
4. Ensure the security and confidentiality of customer non-public information
5. Protect against any anticipated threats or hazards to the security or integrity of sensitive information.
6. Protect against unauthorized access to, or use of, sensitive information.

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 5.3: Common issues found in legal sources that affect Bank-X

In addition, the following tables (Table 5.4: Important issues unique to international legal sources that affect Bank-X and Table 5.5: Important issues unique to local legal sources that affect Bank-X) show a summary of elements unique to the international and local legal sources respectively.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Consumers and customers have the right to “say no” to</td>
<td>1. Data must be retrievable even after long term-</td>
<td>1. Information relating to the financial position, performance, corporate</td>
</tr>
<tr>
<td><strong>GLBA (1999)</strong></td>
<td><strong>SOX (2002)</strong></td>
<td><strong>BASEL II</strong></td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------</td>
<td>--------------</td>
</tr>
<tr>
<td>having their information shared with certain third parties.</td>
<td>retention, even as new technologies are introduced.</td>
<td>governance, risk management and risk exposure of a listed company should be transparent and reliable.</td>
</tr>
<tr>
<td>2. Enable centralized management of data protection policies and enforcement throughout the financial institution.</td>
<td></td>
<td>2. Banks should have an approach for determining what disclosures it will make and the internal controls over the disclosure process.</td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. A financial institute must provide an initial privacy notice to customers not later than the time</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Chapter 5
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.

Table 5.4: Important issues unique to international legal sources that affect Bank-X

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>the relationship commences.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. Reliability and integrity of financial and operating information.
2. Pre- and

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Identify and verify clients</td>
<td>1. Only deal with data collectors that have subscribed to the recorded data protection principles</td>
<td>1. Provides information for banks to follow in order to be regarded as a bank, and</td>
<td></td>
</tr>
<tr>
<td>2. Record all business relations and transactions</td>
<td>2. Consumer information needs to be provided</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
post-implementation reviews have become a key part of successful implementation strategies.

3. Report suspicious and unusual transactions.

3. 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 be allowed to perform banking functions.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>post-implementation reviews have become a key part of successful implementation strategies</td>
<td>.</td>
<td>in order to identify and validate the consumer.</td>
<td>be allowed to perform banking functions.</td>
</tr>
<tr>
<td>.</td>
<td>.</td>
<td>3. Consumers have the right not to be bound to unwanted communications offering goods or services (spam).</td>
<td>.</td>
</tr>
<tr>
<td>3. Report suspicious and unusual transactions.</td>
<td>.</td>
<td>4. If the consumer is bounded, then they must have the option to cancel the subscription to the mailing list.</td>
<td>.</td>
</tr>
<tr>
<td>.</td>
<td>.</td>
<td>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</td>
<td>.</td>
</tr>
</tbody>
</table>

Table 5.5: Important issues unique to local legal sources that affect Bank-X
As mentioned in Chapter 1, it must be emphasized that this analysis of legal sources is not meant to be authoritative. It is intended only to serve the purpose of concept demonstration. Legal advice must be taken from qualified, specialist legal advisers because the author of this dissertation is not a legal expert.

It should further be noted that Tables 5.3 – 5.5 do not show the cross-referencing that would typically be kept with regard to the origin of the legal elements.
5.2.4 Phase 4: Implementation of Solutions

Phase 4, the final phase of the model deals with the implementation of solutions or controls to satisfy the requirements of the legal elements identified during Phase 3. The common and unique elements identified during Phase 3 serve as input to this phase. Bank X is therefore at a stage where solutions can be implemented to ensure compliance with the various legal sources. 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).

It is further important that Bank X ensures that its compliance initiatives dovetail with its security programme. The scenario description in Section 5.1 mentioned basic safeguards like anti-virus solutions, anti-spyware and authentication and access control systems that have been implemented by Bank X. These controls can be listed “against” the legal requirements, where relevant, but can also be cross-referenced to the security programme. A brief and simple example is provided in Table 5.6.

<table>
<thead>
<tr>
<th>Category</th>
<th>Legal Element</th>
<th>Source</th>
<th>Control</th>
<th>Security Programme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy and Protection</td>
<td>Ensure the security and confidentiality of customer non-public information</td>
<td>GLBA, Section 501</td>
<td>Access control systems</td>
<td>ISO 17799, Domain 11</td>
</tr>
</tbody>
</table>

Table 5.6: Cross-Referencing Compliance Controls with Security Initiatives
5.3 Conclusion

In this chapter, an example was used to demonstrate proof-of-concept of the SABS-LeCoM. A limited number of legal sources were used in order for the legal source analysis to be manageable. After conducting the analysis for the proof-of-concept done in this chapter, it became evident that documentation of results would be a very important factor in the success of such a compliance initiative. This was mentioned in the description of the model in Chapter 4. However, it is emphasized here that a database-driven approach should definitely be considered, to facilitate and simplify the compliance process even further.

The utmost importance of linking compliance initiatives with an organization’s security programme should also be stressed here. The process should strive to achieve compliance, but also to optimise organizational resources in using compliance-related controls towards security requirements and vice versa.
FIGURE 5.1: SABS-LECOM – High-Level Diagrammatic Representation

Legal sources

Investigation of Legal sources

Identification of Elements

Common Elements

Unique Elements

IMPLEMENTATION OF SOLUTIONS

Selected Legal sources affecting the South African Financial Sector

* Sarbanes-Oxley Act
* King Report
* Gramm-Leach-Bliely Act
* ECT Act
* Basel Capital Accord
* And many more
6.1 Introduction

In this chapter, the research presented in this dissertation is concluded. Chapter 6 provides an overview of how the objectives of the research were met throughout the dissertation. The benefits of the SABS-LeCoM are revisited and some areas suitable for future research are also suggested.

At the commencement of this research project, the South African banking sector was analysed from an information security perspective. Through studying the banking sector, it was realised that there are issues that arise with information that is held by the banking sector. This information is very important and any covert manipulation of the information can harm the identity of the bank and cause loss of trust from its clients.

The banking sector carries important information about their clients and their accounts. Nowadays, with technology advancement, it is very dangerous not to ensure that such information is secured. The information needs to be secured from threats that can damage it. There are various guidelines that can direct efforts to protect and safeguard information held by banks. International standards, best practices guidelines and legal sources are good examples of such guidelines.

There are various legal sources that can be used to aid in the securing of financial information. The fact is, however, that becoming compliant with any of the myriad regulations affecting organizations can’t be achieved in a single epochal event because there’s simply too much to do (Mazer, 2007). As
supported by Mazer (2007), there are a vast number of legal sources and requirements to consider. Mazer further states that compliance with these legal sources cannot be solved by revising business processes or deploying new technology (Mazer, 2007) only. To complicate matters even more, most of the legal sources are vague and not easily readable. SOX is a good example of a law that is well-known for its vagueness.

Financial institutions consequently find themselves saddled with a potpourri of legal sources and vague requirements. If such institutions operate in a reactive mode, they may find themselves wasting valuable resources on disjointed compliances projects, each racing towards a compliance deadline. Therefore this research investigated a solution for this problem and proposed a regulatory compliance model called the South African Banking Sector Legal Compliance Model (SABS-LeCoM) for financial institutions to address the situation coherently and in a proactive way.

### 6.2 Benefits of the SABS-LeCoM

The benefits of the SABS-LeCoM were listed in Section 4.3 of Chapter 4. In this section, each of the benefits listed in Section 4.3 is revisited and briefly discussed.

#### 6.2.1 Compliance management for multiple legal sources rather than individual laws

The model ensures that identified legal sources are managed into a single view. Therefore, whenever there is a new legal source, it is easier to add any new requirements without compromising the existing requirements that still need to be complied with. The legal sources will be managed easily without the risk of losing any of the existing or new requirements. The context of
compliance changes over time; new regulations emerge, existing ones receive new interpretation, and the organization’s own business and technology environments change, all of which require re-examination and potential improvement of current controls (Mazer, 2007). This underscores the importance of the structured approach proposed by the SABS-LeCoM. It simply is not a viable option to address legal requirements in the context of each individual legal source only.

6.2.2 Optimization of resources

Due to the proliferation in legal sources, financial institutions have to commit a lot of organization resources to ensure compliance. Gartner Group research shows that organizations spend as much money on compliance as they do on security: between 3-6% of their IT budgets for each (Getronics, 2005). The identification of legal sources and requirements to comply with, for any business, is a tedious task. This task requires organizations to find the necessary resources that will identify and analyse the relevant legal sources to comply with. The SABS-LeCoM proposes that with a central view of legal source requirements, less time, money and people will be required to implement and maintain a unified compliance approach.

6.2.3 Elimination of redundancies found in various legal sources

As more legal sources are identified, the SABS-LeCoM ensures that the previously identified requirements are in a single view. Therefore, whenever there are new requirements to comply with, the SABS-LeCoM provides a way of ensuring that the new requirements do not overlap with existing requirements.
6.2.4 Reduction in overall compliance monitoring effort

The model ensures that less time is spent gathering legal sources and trying to identify the requirements to be used for securing information. This is done by providing a single view of legal requirements. It also ensures that solutions (controls) that have already been implemented, can be used towards complying with the requirements of various legal sources.

6.2.5 Combination of efforts and resources towards security initiatives, with legal compliance efforts

Organizations can address both compliance and regular security maintenance needs simultaneously, and do so without irrational spending (Getronics, 2005). The SABS-LeCoM fits right into this approach by ensuring in Phase 4 of the model, that implemented solutions or controls, are cross-referenced both to legal sources and security initiatives.

6.3 Chapter Overview

This section aims at providing a summary of the research conducted throughout this study and shows how the objectives of the research were met. Since one sub-objective of the research was typically addressed in each of Chapters 2 – 5, the discussion of the chapters is aligned with these sub-objectives, except for Chapter 1 and Chapter 6, which respectively introduces and concludes the research.

6.3.1 Chapter 1 - Introduction

Chapter 1 starts off by motivating the importance of protecting financial information from fraudulent behaviour by providing examples of two corporate
fraud organizations and how they became notorious in the business world. The chapter stated the problem statement, objectives, and the methodology used to meet these particular objectives.

6.3.2 Chapter 2 – South African Financial Institutions and Financial Information Security

Sub-Objective 1

- Investigate the current state of the South African financial sector and the importance of securing financial information.

In the past five years, issues such as corporate governance, integrity of credit card data, and consumer data privacy have forced companies to devote substantial attention and resources to meeting these new challenges (Mazer, 2007). Chapter 2 addressed the South African financial industry and mechanisms that can be used to protect financial information. Chapter 2 was aimed at awareness of the security issues related to the financial industry and the impact technology has on securing information.

Finally, it noted that the financial industry faces increasing internal control challenges as legal sources and industry guidelines affect daily operations. Therefore, compliance issues have progressively gained importance on the corporate agenda. However, the legal sources do not specify how to secure information, thus increasing the confusion in businesses.

6.3.3 Chapter 3 – Legal Sources

Sub-Objective 2
• An investigation of the legal sources that influence financial institutions in securing information, in particular, in the South African financial sector.

Many countries have systems to regulate and supervise banks and other financial services, in order to prevent that the risks taken by the financial industry would have negative effects on society (Stichele, 2004). Legal sources are needed to regulate the protection of information. Chapter 3 started off by explaining the importance of legal sources within organizations. Furthermore, the impact of legal sources on IT operations within financial services was also discussed, in order to understand the influence legal sources have on financial services and financial information. A brief overview of legal sources and the impact it has on the South African financial sector was provided. The chapter concluded that a compliance model is needed that will aid the financial sector through managing the legal sources that must be complied with.

6.3.4 Chapter 4 – A Model for Legal Compliance in the South African Banking Sector.

Sub-Objective 3

• Finding a way to consolidate the requirements of various legal sources that influence the South African financial sector.

Chapter 4 provided a brief overview of the importance of having a compliance model in order to aid organizations (financial services) to comply with legal sources that affect their line of business. Furthermore, the South African Banking Sector Legal Compliance Model (SABS-LeCoM) was explained and how it can be utilized to aid in identifying requirements to protect financial information.
The concept behind the model is to provide a single view of legal sources that affect the financial sector. Additionally, the compliance model minimizes the complexity of complying with more than one legal source. The model was designed to decrease, if not eliminate, the redundancy of complying with legal source elements that are covered in different legal sources.

6.3.5 Chapter 5 – SABS-LeCoM: Proof of Concept Using Privacy and Internal Controls

Sub-Objective 4

- The provision of an information security model for regulatory compliance from the perspective of the South African financial sector

Chapter 5 was dedicated to applying the compliance model that was proposed in Chapter 4 through providing a case study of legal sources affecting the South African banking sector as a proof of concept. A fictional scenario of a South African bank (Bank X) was described. This scenario was used to illustrate how the phases of the SABS-LeCoM will be executed in attempting a unified compliance approach based on the model.

6.3.6 Chapter 6 – Conclusion

The conclusion of the research is done in this chapter. The benefits of the SABS-LeCoM are revisited and a chapter overview is presented and aligned with the achievement of the objectives of the research. The chapter concludes with a discussion of possible future research projects to address areas outside of the scope of this dissertation.
6.4 Future Research

The SABS-LeCoM presented in this dissertation has a number of benefits as already discussed in Section 6.2. The creation of this solution was, however, subject to issues as determined by the scope limitations of this research (refer to Chapter 1, Section 1.6). A number of future research projects can therefore be proposed.

It would firstly be of benefit to apply the model in a practical situation (i.e. at a South African bank), to identify possible improvements to the model which can then be tested again in a second iteration of the model.

Secondly, the information security milieu at a particular institution is multidimensional and comprises various issues and security initiatives. It would be of value to investigate the link between the SABS-LeCoM which primarily addresses the legal dimension, and the other dimensions of security in more depth.

Thirdly, it was stated previously that this research has been conducted from the perspective of information security and that the researcher is not a legal expert. Certainly, it would be beneficial to further this project through incorporation of the inputs of legal experts, who would be able to add further insight into the handling of the legal requirements.
6.5 Conclusion

In this chapter, it was illustrated that all the objectives that were established at the beginning of this research project, were accomplished. The information covered in various chapters of the dissertation was reviewed and ideas for future research were discussed.

By maintaining a strategic perspective, it is possible to institutionalize legal compliance as well as security initiatives at a company-wide level, if the approach promoted by the SABS-LeCoM is adopted. As more legal sources emerge which impact on the protection of information, it will become even more important for organizations to follow a unified, consistent approach to legal compliance.

Aimes, F., 2005, It’s the law, and more, Brainstorm Special Focus – An independent report, Brainstorm vol. 4 issue 10, pp 22-24


BMI TechKnowledge Group, Sited: 29 Jul. 05, AVAILABLE ON THE INTERNET: http://www.bmi-t.co.za/bmi/web-files/focus-areas/banking.htm


Business Report, 2004, Financial compliance driving IT investment, Date: 5 Nov 2004,


Captaris, 2005, The Impact of Regulations on Archiving, Sited: 12 Aug 2005,
AVAILABLE ON THE INTERNET: http://www.bitpipe.com/detail/RES/1118242071_890.html


Citrix System, (January 2004), Regulatory Compliance Demands Secure Access to Information: Access Infrastructure – Technology for Access Control, Security and
Oversight – Citrix Infrastructure Solutions, Sited: 27 Jul 2005, AVAILABLE ON THE INTERNET:

http://www.emc.com/analyst/pdf/Cohasset_CorpGovWP.pdf

Committee of Sponsoring Organisations, 1992, Internal Control – Integrated Framework. (COSO)

Conner, F. W., Coviello, A. W., April 2004, Information Security Governance: Corporate Governance Report, Sited: , AVAILABLE ON THE INTERNET:
http://www.cyberpartnership.org/InfoSecGov4_04.pdf


http://www.continuitycentral.com/feature0210.htm


http://www.deloitte.com/dtt/cda/doc/content/DTT_DR_ProsSecFull_Sept2004.pdf


References


Esselaar, P., 2007, Conversation through e-mail with the Korbitec’s IT Law Manager. 18 June 2007.


Hinson, G., (January 2005), Proposing the role of “Governance Director” or “Chief Governance Officer” (CGO), AVAILABLE ON THE INTERNET:


Information Builders, (January 2004), Achieving Compliance: Meeting Today's Reporting Requirements With Business Intelligence Technology, Sited: 03 June 2005, AVAILABLE ON THE INTERNET:

IT Governance Institute, 2004, IT Control Objectives for Sarbanes-Oxley, Date: Apr 2004, Cited: 8 Feb 2005, AVAILABLE ON THE INTERNET:
http://www.itgi.org/Template_ITGI.cfm?Section=ITGI&CONTENTID=9757&TEMPLATE=/ContentManagement/ContentDisplay.cfm

http://whitepapers.businessweek.com/data/detail?id=1100713634_390&type=RES&src=TOPRES

http://www.windowsitlibrary.com/Content/1234/03/1.html


http://www.vnh.co.za/news_legal_view?mode=content&id=17497


Loyd, S., (March 2004), Corporate Governance and Information Security: An analysis of increased interest in Information Security within today’s Boardroom,


MetaGroup, 2005, Unravelling Security and Risk Regulation,


Plotkin, J, 2003, Corporate Governance – The Impact on Your IT Staff, Date: 5 Sep 2003, Cited: 14 Feb 2005, AVAILABLE ON THE INTERNET:


INTERNET:
http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=15998


Smith, R., n.d., Sarbanes-Oxley Act and IT: Why There is No ‘I’ in ‘SOX Team’, Sited: 25 May, AVAILABLE ON THE INTERNET:
http://www.integrationconsortium.org/docs/Sarbanes_Oxley/There_Is_No_I_In_Sarbanes_Oxley_Team.pdf


Sophos®, (December 2004), Effective Compliance Practice: Information security, email security, proof of control, Sited: 07 Feb. 2005, AVAILABLE ON THE INTERNET:


Stralser, S., 2004, MBA in a Day: What You Would Learn at Top-Tier Business Schools (If you only had the time), John Wiley & Sons, Inc., Hoboken, New Jersey


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


TOWARDS REGULATORY COMPLIANCE

- A MODEL FOR THE SOUTH AFRICAN FINANCIAL SECTOR –

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
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.

IMPORTANT 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 utmost 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.

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.

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.

**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.

**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:

5. Regulation identification
6. Identification of sections relevant to the securing of information
7. Assessment of sections (to identify common and unique elements)
8. 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.
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.

**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.

**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**

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

**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:

**Review Elements**

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

**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.

**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.

**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.
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

<table>
<thead>
<tr>
<th>Privacy and Protection</th>
<th>Identification, reviews and assurance reporting of internal controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>7. Safeguarding of assets</td>
<td>7. A statement of management’s responsibility is needed for establishing and maintaining adequate internal control over financial reporting.</td>
</tr>
<tr>
<td>8. Assurance on the effectiveness and efficiency of operations within the organization</td>
<td>8. A statement is needed for identifying the</td>
</tr>
<tr>
<td>Privacy and Protection</td>
<td>Identification, reviews and assurance reporting of internal controls</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>9. A financial institute must provide an initial privacy notice to customers not later than the time the relationship commences.</td>
<td>framework used by management to evaluate the effectiveness of the company's internal control over financial reporting.</td>
</tr>
<tr>
<td>10. Location where the media is stored must be highly controlled.</td>
<td>9. Rehearsals and reviews on a regular basis are necessary to ensure that plans are continuing to meet compliance objectives</td>
</tr>
<tr>
<td>11. Ensure the security and confidentiality of customer non-public information</td>
<td>10. Assurance on the effectiveness and efficiency of operations within the organization needs to be completed.</td>
</tr>
<tr>
<td>12. Protect against any anticipated threats or hazards to the security or integrity of sensitive information.</td>
<td>11. External auditor must attest the effectiveness of internal controls each year, based on reliable evidence</td>
</tr>
<tr>
<td>13. Protect against unauthorized access to, or use of, sensitive information.</td>
<td>12. The directors have a responsibility to ensure that an effective internal control is being maintained</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6. Consumers and customers have the right to “say no” to having their information shared with certain third parties.</td>
<td>2. Data must be retrievable even after long term-retention, even as new technologies are introduced.</td>
<td>3. Information relating to the financial position, performance, corporate governance, risk management and risk exposure of a listed company should be transparent and reliable.</td>
</tr>
<tr>
<td>7. Enable centralized management of data protection policies and enforcement throughout the financial institution.</td>
<td></td>
<td>4. Banks should have an approach for determining what disclosures it will make and the internal controls over the disclosure process.</td>
</tr>
<tr>
<td>8. If the financial institution wants to disclose information in a way not described on its privacy policy, a revised privacy policy may be required.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. A financial institute must provide an initial privacy notice to customers not later than the time the relationship commences.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10. Review the encryption standards used by the</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------</td>
<td>------------</td>
<td>----------</td>
</tr>
<tr>
<td>institution. The selection of data to encrypt and the encryption technique and level should be supported by the risk assessment.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>3. Reliability and integrity of financial and operating information.</td>
<td>4. Identify and verify clients</td>
<td>6. Only deal with data collectors that have subscribed to the recorded data protection principles</td>
<td>2. Provides information for banks to follow in order to be regarded as a bank, and be allowed to perform banking functions.</td>
</tr>
<tr>
<td>4. Pre- and post-implementation reviews have become a key part of successful implementation on strategies</td>
<td>5. Record all business relations and transactions.</td>
<td>7. Consumer information needs to be provided in order to identify and validate the consumer.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. Report suspicious and unusual transactions.</td>
<td>8. Consumers have the right not to be bound to unwanted communications offering goods or services (spam).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>9. If the consumer is bounded, then they must have the option to cancel the subscription to the mailing list.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>10. 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</td>
<td></td>
</tr>
</tbody>
</table>

**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.

REFERENCES


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