A Gap Analysis to Compare Best Practice Recommendations and Legal Requirements when raising Information Security Awareness amongst Home Users of Online Banking

Carla-Lee Botha

A Gap Analysis to Compare Best Practice Recommendations and Legal Requirements when raising Information Security Awareness amongst Home Users of Online Banking

By

Carla-Lee Botha

Submitted in accordance with the requirements
for the degree of

Master of Science

in the subject

Information Systems

at the

UNIVERSITY OF SOUTH AFRICA

Supervisor: Marianne Loock
Co-supervisor: Dr Elmarie Kritzinger

June 2011

Declaration

Student Number: 47191260

I declare that *A Gap Analysis to Compare Best Practice Recommendations and Legal Requirements when raising Information Security Awareness amongst Home Users of Online Banking* is my own work and that all the resources that I have used or quoted have been indicated and acknowledged in my References.

Carla-Lee Botha_____ 08/06/2011_____
Name Date

_____
Signature

Abstract

South African home users of the Internet use the Internet to perform various everyday functions. These functions include, but are not limited to, online shopping, online gaming, social networking and online banking. Home users of online banking face multiple threats, such as phishing and social engineering. These threats come from hackers attempting to obtain confidential information, such as online banking authentication credentials, from home users. It is, thus, essential that home users of online banking be made aware of these threats, how to identify them and what countermeasures to implement to protect themselves from hackers. In this respect, information security awareness (ISA) programmes are an effective way of making the home users of online banking aware of both the threats they face and the countermeasures available to protect themselves from these threats.

There are certain legal requirements with which South African banks have to comply when implementing ISA initiatives. Non-compliance or failure to demonstrate due care and due diligence should a security incident occur will result in financial penalties for the bank as well as possible brand damage and loss of customers. Banks implement international best practice recommendations in an effort to comply with legislation. These include recommendations for information security awareness.

This research investigated both information security best practice recommendations and information security legal requirements for information security awareness. A selected list of information security best practices was investigated for best practice recommendations while a selected list of information security legislation was investigated for legal requirements imposed on South African banks. A gap analysis was performed on both these recommendations and requirements to determine whether the implementation of best practice recommendations resulted in compliance with legal requirements. The gap analysis found that the implementation of best practice recommendations does not result in compliance with legal requirements. Accordingly, the outcome of this research highlighted the importance of understanding the legal requirements and ensuring that adequate controls are in place with which to achieve compliance.

Acknowledgements

This dissertation would not have been possible without the help of a number of important people. Thank you, firstly, to my Dad, Mom and Colin Miles for their on-going support of my decision to do my Masters. Also, to the Soals who made it possible in the early days. Thank you to Janet Critchlow, who herself has done her Masters, for helpful advice on how to cope with the occasionally frustrating process. Thank you to Mra Khwar Nyo for her patience with my spontaneous and often vague questions. To my Supervisors, Marianne Loock and Dr Elmarie Kritzinger, I could not have asked for better Supervisors. Their clear direction setting and positive attitude always kept me on track and moving forward. Last, but not least, to Dan for all his love and support.

1 INTRODUCTION 1

1.1 INTRODUCTION 2
1.2 PROBLEM STATEMENT 3
1.3 OBJECTIVE OF THE RESEARCH 4
1.4 APPROACH 4
1.5 DELINEATION OF SCOPE 5
1.6 DELIVERABLES 6
1.7 DEFINITIONS 6
1.8 DISSERTATION STRUCTURE 7

2 INFORMATION SECURITY AWARENESS PROGRAMMES IN BANKS 9

2.1 INTRODUCTION 11
2.2 CONTEXT OF THE RESEARCH 12
2.2.1 Information Security Awareness Programme 12
2.2.2 Home Users 12
2.2.3 Online Banking 13
2.2.4 Background to the Research 13
2.3 CURRENT ISA PROGRAMME DEVELOPMENT AND ASSESSMENT INSTRUMENTS 16
2.3.1 Da Veiga & Eloff (2010) 17
2.3.2 Kruger & Kearney (2006); Kelly (2006); Wiederkehr (2003); Hansche (2001); Albrechtsen & Hovden (2009) 18
2.3.3 Taylor & Shepherd (2007) 20
2.3.4 May (2008); McKenna (2009); Siponen (2000) 20
2.3.5 Desman (2002); ENISA (2006) 21
2.3.6 Kruger & Kearney (2008) 21
2.3.7 Valentine (2006) 22
2.3.8 Siponen (2001) 22
2.3.9 Rotvold (2008) 23
2.3.10 Peltier (2005) 23
2.3.11 Wiles, Claypoole, Henry, Drake & Lowther (2008) 23
2.4 ACCEPTANCE OF ONLINE BANKING 24
2.5 SUMMARY 25

3 CURRENT AND PREVALENT THREATS TO ONLINE BANKERS 27

3.1 INTRODUCTION 29
3.2 DOCUMENTS TO BE ANALYSED 30
3.3 NARROWING THE LIST TO A "TOP 10" 32
3.4 BUILDING THE THREAT LIST 33
3.4.1 SANS 33
3.4.2 National Cyber Security Alliance 39
3.4.3 CSOOnline 41
3.4.4 CIO 42
3.4.5 Bankinfosecurity 44
3.4.6 Elsevier Academic Papers 47
3.5 THE TOP 10 LIST 49
3.6 SUMMARY 51

4 INFORMATION SECURITY AWARENESS BEST PRACTICE 52

4.1 INTRODUCTION 54
4.2 DOCUMENTS TO BE ANALYSED 54
4.3 COMPILING THE BEST PRACTICE RECOMMENDATIONS LIST 55
4.3.1 COBIT 4.1 56
4.3.2 ISO/IEC 27001 61
4.3.3 The Standard of Good Practice for Information Security 65
4.4 THE BEST PRACTICE RECOMMENDATIONS LIST 72
4.5 SUMMARY 75

5 INFORMATION SECURITY AWARENESS LEGISLATION 76

5.1 INTRODUCTION 78
5.2 DOCUMENTS TO BE ANALYSED 78
5.3 COMPILING THE LEGAL REQUIREMENTS LIST 80
5.3.1 BASEL II 81
5.3.2 Sarbanes-Oxley Act of 2002 85
5.3.3 Gramm-Leach-Bliley Act of 1999 88
5.3.4 Electronic Communications and Transactions Act, 2002 91
5.3.5 Protection of Personal Information Bill, 2009 92
5.3.6 Promotion of Access to Information Act, 2000 94
5.3.7 The Code of Banking Practice 95
5.3.8 Consumer Protection Act, 2008 97
5.3.9 Constitution of the Republic of South Africa 98
5.3.10 Code of Governance Principles for South Africa (King III), 25 February, 2009 99
5.3.11 Electronic Communications Act, 2005 100
5.4 THE LEGISLATION REQUIREMENTS LIST 101
5.5 SUMMARY 109

6 THE GAP BETWEEN BEST PRACTICE RECOMMENDATIONS AND LEGAL REQUIREMENTS 110

6.1 INTRODUCTION 112
6.2 COMPARISON OF LEGAL REQUIREMENTS AND BEST PRACTICE RECOMMENDATIONS 112
6.3 FINDINGS 117
6.4 SUMMARY 118

7 CONCLUSION AND RECOMMENDATIONS 119

7.1 INTRODUCTION 121
7.2 SCOPE OF RESEARCH 121
7.3 PROBLEM AREAS IDENTIFIED THROUGH THE RESEARCH 122
7.3.1 The Gap 122
7.3.2 Limited Number of Best Practice Standards Included 122
7.3.3 Legislation is Open to Interpretation 122
7.3.4 The Provision for Evolving Threats in Legislation 122
7.3.5 Validation of Research Findings 123
7.4 RESEARCH QUESTIONS 123
7.4.1 Information Security Best Practice 123
7.4.2 Information Security Legislation 123
7.4.3 Identifying the Gap 124
7.4.4 The Problem Statement 124
7.5 FUTURE WORK 124
7.6 SUMMARY 125

8 REFERENCES USED IN TEXT 127

9 REFERENCES NOT USED IN TEXT 137

10 ARTICLE SUBMITTED TO ISSA 2011 141

LIST OF TABLES

TABLE 3-1 INFORMATION SECURITY THREAT TERMINOLOGY 29
TABLE 3-2 SANS THREATS 34
TABLE 3-3 NCSA THREATS 39
TABLE 3-4 CSOONLINE THREATS 40
TABLE 3-5 CIO THREATS 42
TABLE 3-6 BANKINFOSECURITY THREATS 44
TABLE 3-7 ELSEVIER THREATS 47
TABLE 3-8 THREAT SUMMARY 49
TABLE 4-1 COBIT 4.1 RECOMMENDATIONS 57
TABLE 4-2 ISO/IEC 27001 RECOMMENDATIONS 62
TABLE 4-3 THE STANDARD OF GOOD PRACTICE FOR INFORMATION SECURITY RECOMMENDATIONS 66
TABLE 4-4 BEST PRACTICE RECOMMENDATIONS SUMMARY 72
TABLE 5-1 BASEL II REQUIREMENTS 81
TABLE 5-2 SARBANES-OXLEY ACT OF 2002 REQUIREMENTS 86
TABLE 5-3 THE GRAMM-LEACH-BLILEY ACT OF 1999 REQUIREMENTS 89
TABLE 5-4 ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT, 2002 REQUIREMENTS 90
TABLE 5-5 PROTECTION OF PERSONAL INFORMATION BILL, 2009 REQUIREMENTS 92
TABLE 5-6 PROMOTION OF ACCESS TO INFORMATION ACT, 2000 REQUIREMENTS 93
TABLE 5-7 CODE OF BANKING PRACTICE REQUIREMENTS 95
TABLE 5-8 CONSUMER PROTECTION ACT, 2008 REQUIREMENTS 96
TABLE 5-9 CONSTITUTION OF THE REPUBLIC OF SOUTH AFRICA REQUIREMENTS 97
TABLE 5-10 CODE OF GOVERNANCE PRINCIPLES FOR SOUTH AFRICA (KING III), 2009 REQUIREMENTS 98
TABLE 5-11 ELECTRONIC COMMUNICATIONS ACT, 2005 REQUIREMENTS 99
TABLE 5-12 LEGAL REQUIREMENTS 103

LIST OF FIGURES

FIGURE 1-1 DISSERTATION STRUCTURE 6
FIGURE 2-1 CRITICAL ELEMENTS OF A SECURITY AWARENESS AND TRAINING PROGRAMME 11
FIGURE 6-1 COMPARISON OF LEGAL REQUIREMENTS AND BEST PRACTICE RECOMMENDATIONS 115

Chapter 1:

Introduction

1.1 Introduction

South Africans use the Internet for business purposes and at home. Home users, who have access to the Internet, use the Internet to perform various functions on a daily basis. These functions include online shopping, online gaming, social networking and online banking. Online banking is a convenient way in which to carry out banking tasks, such as managing bank accounts, checking an account transaction history, transferring money and paying bills. Online banking eliminates the need to travel to a bank each time the customer has to complete a transaction. Online banking gives individuals the option to bank in the comfort of their own homes. While convenient, home users face multiple threats when online banking, such as phishing and social engineering. These threats emanate from hackers attempting to obtain confidential information from home users, for example, online banking authentication credentials. It is, thus, essential that the home users of online banking be made aware of these threats, how to identify them and the countermeasures available to protect themselves from the hackers' attempts.

By definition, online banking is a system which allows home users to conduct their banking over the Internet (Investorwords, 2011). Online banking may also be defined as a service which consumers use to conduct financial transactions in a secure manner via a website operated by their banks (Wikipedia, 2011[a]). Cell phone banking is also a convenient alternative form of banking. This form of banking makes use of a cell phone to enable users to perform several of the tasks they would normally perform in the course of online banking, for example, viewing account balances, transferring money and paying accounts (Birch, 1999). Both online and cell phone banking have already become the subject of numerous international studies (Al-Somali, Gholami & Clegg, 2009; Lassar, Manolis & Lassar, 2005; Pikkarainen, Pikkarainen, Karjaluoto & Pahnila, 2004; Sathye, 1999; Sadique Sohail & Shanmugham, 2003). In addition, there have also been studies carried out on online and cell phone banking in the African context (Brown, Cajee, Davies & Stroebel, 2003; Gikandi & Bloor, 2009; Porteous, 2006). This research focuses on online banking by home users in a South African context. The research recognises the following needs:

- the need for South African banks to protect their home users from the threats they face as online bankers (Albrechtsen & Hovden 2009; Da Veiga & Eloff, 2010; Siponen, 2001; Wiederkehr, 2003)
- the need for South African banks to demonstrate both due care and due diligence when addressing the threats faced by their home user base by implementing best practice (Da Veiga & Eloff, 2010; Siponen, 2001; Wiederkehr, 2003)
- the need for South African banks to take cognisance of both the legal and regulatory requirements imposed on them and the importance of compliance with these requirements (Da Veiga & Eloff, 2010; Hansche, 2001; Siponen, 2001)

These needs form the basis of this investigation.

1.2 Problem Statement

It is incumbent on banks to satisfy certain legal requirements. Banks are able to draw on information security best practices when implementing an information security awareness (ISA) programme. The problem statement is therefore as follows:

> South African home users of online banking need to be informed on how they can protect themselves from losing sensitive personal information to malicious hackers. South African banks need to demonstrate due diligence and due care, not only to help these home users protect themselves from current threats, but to also comply with applicable laws and regulations. Banks can implement best practice controls in an effort to achieve this. This investigation sets out to determine whether implementing information security awareness best practices results in automatic compliance with information security awareness laws and regulations.

The research question and sub-questions addressed by this investigation include the following:

- In an attempt to protect home users of online banking from current threats, would the implementation of information security awareness best practices by South African banks automatically result in due diligence and due care requirements imposed by information security awareness legislation?

    - What are the current threats faced by home users of online banking?
    - What are the information security best practice recommendations for information security awareness of home users of online banking?
    - What are the information security legal requirements imposed on South African banks in respect of information security awareness for their home users of online banking?
    - Is there a gap between information security best practice recommendations and existing information security legal requirements?

These questions guided the research in determining whether the implementation of ISA best practice will result in compliance with ISA legal requirements.

1.3 Objective of the Research

The objective of this research is to investigate whether a gap exists between the legal requirements imposed on banks for ISA programmes aimed at the home users of online banking and recommendations offered by information security best practice for such programmes. Accordingly, this investigation will help determine whether implementing ISA best practice necessarily results in compliance with ISA laws and regulations.

1.4 Approach

This research sets out to compare ISA best practice recommendations and ISA legal requirements in order to determine whether a gap does, indeed, exist. Selected information security best practices are analysed for recommendations for

implementation of an ISA programme aimed at the home users of online banking. In addition, selected information security legislation pertinent to South African banks is analysed for requirements imposed on South African banks when implementing an ISA programme aimed at the home users of online banking. The ISA best practice recommendations identified are then compared with the ISA legal requirements identified and any possible gap between the two noted. For the remainder of this research, ISA best practice and ISA legislation will be referred to as best practice and legislation respectively.

1.5 Delineation of Scope

Documents were selected based on criteria described in the relevant chapters. Although other widely-accepted international standards exist, such as ITIL, these were excluded as they make reference to the need for security and security management within their broader scope, but do not offer detail on security controls.

The best practices or international standards identified include the following:

- COBIT (Version 4.1)
- ISO/IEC 27001
- Standard of Good Practice for Information Security (2007)

The legislation identified for this study includes the following:

- Basel II
- Sarbanes-Oxley Act of 2002
- Gramm-Leach-Bliley Act of 1999
- Electronic Communications and Transactions Act, 2002
- Protection of Personal Information Bill
- Promotion of Access to Information Act, 2000
- The Code of Banking Practice
- Consumer Protection Act, 2008
- Constitution of the Republic of South Africa

- Code of Governance Principles for South Africa (King III), 25 February, 2009
- Electronic Communications Act, 2005

1.6 Deliverables

This dissertation makes a contribution towards research within the information security area while focusing on legislation and best practice for information security awareness. The researcher carried out a gap analysis on the legal requirements and the best practice recommendations for information security awareness aimed at the home users of online banking. The findings of this gap analysis are presented. The gap identified between best practice recommendations and legal requirements may serve as a basis for future investigations into the reasons why this gap exists and proposals to close this gap.

1.7 Definitions

Term	Definition
Law	Rule or system of rules imposed by a government to regulate society and normally carry consequences for noncompliance (*Cambridge Dictionaries Online*, 2011[a]; *Oxford English Dictionaries*, 2011[a])
Regulation	Official rule imposed and maintained by a relevant authority (*Cambridge Dictionaries Online*, 2011[b]; *Oxford English Dictionaries*, 2011[c])
Statute	A statute is a written law, such as an Act, which has been formally passed by a legislative body (*Cambridge Dictionaries Online*, 2011[c]; *Oxford English Dictionaries*, 2011[d]).
Contractual obligation	Deeds a party is obliged to perform, as stated in a contract (*Cambridge Dictionaries Online*, 2011[d])
Best practice	A best practice is a procedure or method which is known to achieve the best possible results (BusinessDictionary, 2011; Methods & Tools QA Resources, 2009; Wikipedia, 2011[b])

1.8 Dissertation Structure

Figure 1-1 depicts an overview of the dissertation.

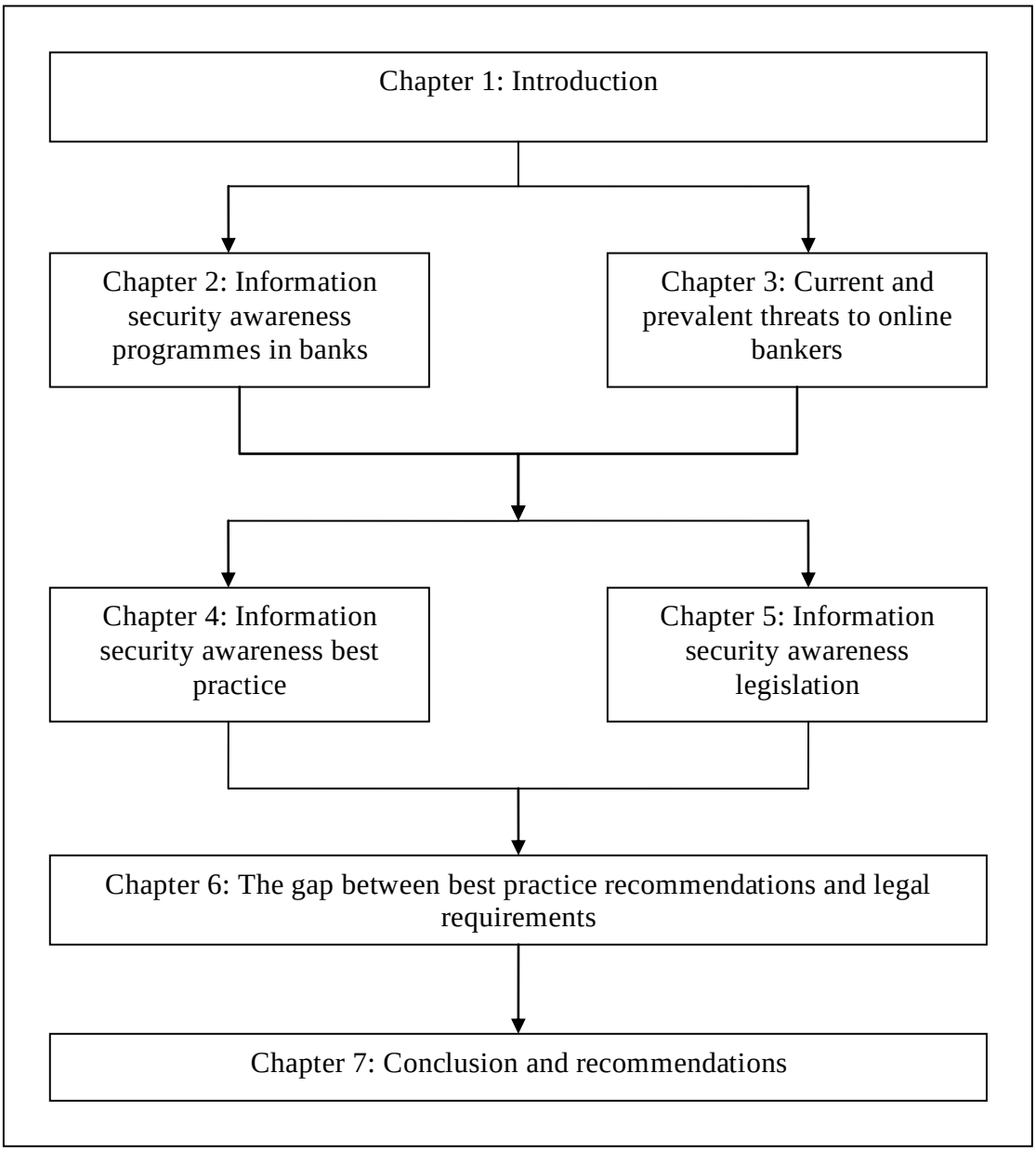


Figure 1-1 Dissertation structure

The dissertation comprises seven chapters. Chapter 1 defines the problem statement and presents the research questions.

Chapter 2 places the research in context by means of a literature study carried out on previous research into ISA programmes.

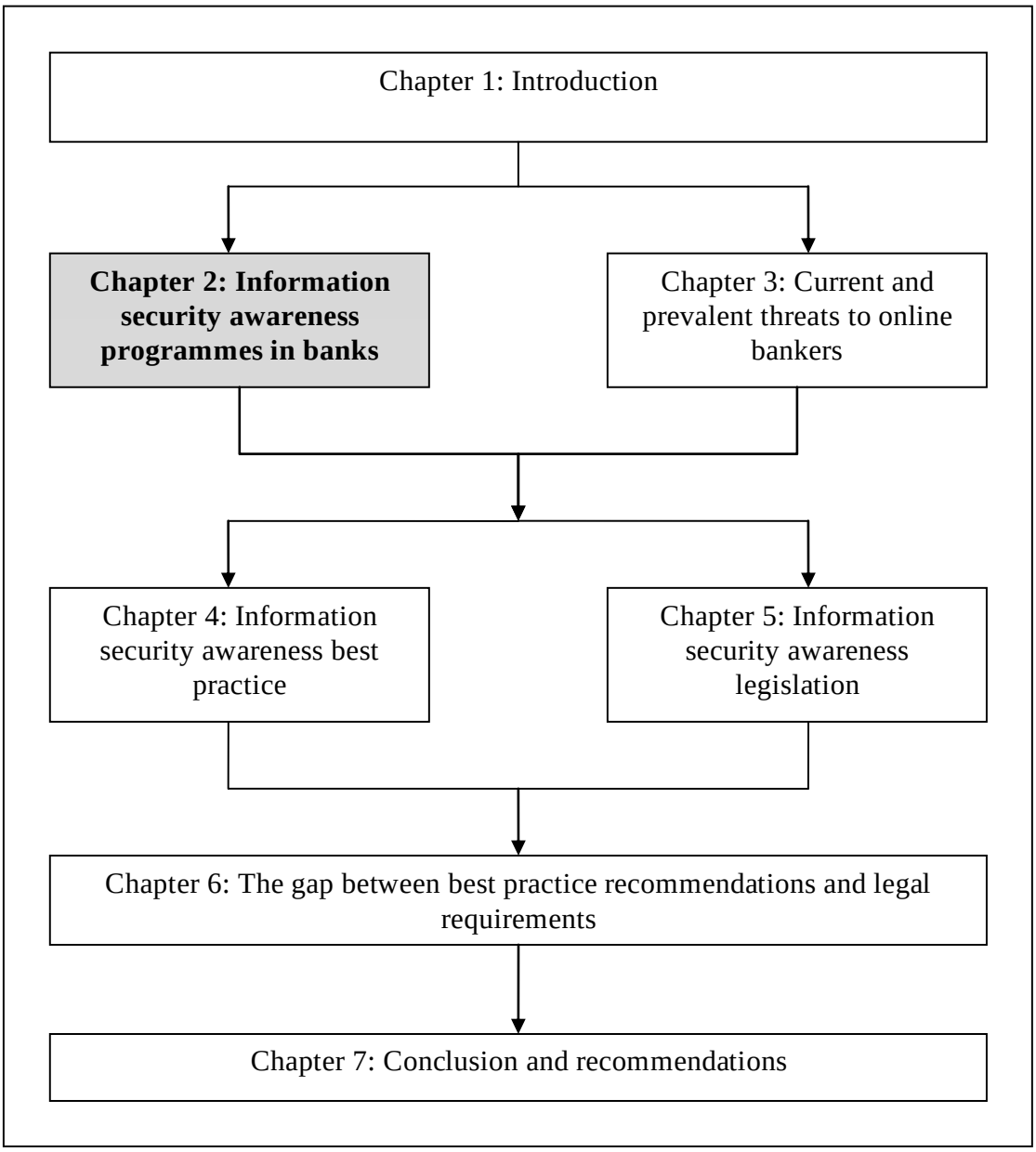
Chapter 3 identifies the current and most prevalent information security threats facing the home users of online banking – the very reasons why it is essential that security initiatives be in place. Up-to-date electronic sources are investigated for the latest information security threats as well as tips on ways in which to counter these threats. Recent statistics on information security threats will be analysed to ascertain the most prevalent information security threats.

Chapters 4 and 5 identify ISA recommendations and requirements by analysing a list of both selected international best practices and selected laws and regulations pertinent to information security in South African banks. Chapter 6 compares these recommendations and requirements and succeeds in identifying a gap.

Finally, Chapter 7 concludes the research by revisiting both the problem statement and the research questions. Chapter 7 also offers recommendations for future research.

Chapter 2:

Information Security Awareness Programmes in Banks


Chapter 1: Introduction
Chapter 2: Information security awareness programmes in banks
Chapter 3: Current and prevalent threats to online bankers
Chapter 4: Information security awareness best practice
Chapter 5: Information security awareness legislation
Chapter 6: The gap between best practice recommendations and legal requirements
Chapter 7: Conclusion and recommendations

2.1 Introduction

Information security awareness (ISA) comprises one component of an information security programme and it is associated with the education of the end users of an information technology system on relevant information security threats and countermeasures. This research addresses the responsibilities incumbent on South African banks for the information security awareness of South African home users of online banking. This chapter discusses the background to the research topic and places the focus of the research in context.

The literature study in this research comprises two parts. The first part addresses current ISA programme development and assessment instruments. Literature on ISA programme development and assessment instruments is identified in prominent electronic academic journals and databases. The purpose of the first part of the literature study is to investigate what guidance can be drawn from available literature for ISA programme development. The second part of the literature study reviews factors which affect the acceptance of online banking by users to ascertain what users perceive as obstacles to their acceptance of online banking. Literature on the acceptance of online banking is identified in prominent electronic academic journals and databases. International studies are also included in the survey. The purpose of the second part of the literature study is to identify factors affecting the acceptance of online banking in order to gain an insight into users' perceptions of the online banking service. An understanding of factors which prevent the end user from accepting online banking may shape the content of an ISA programme to demonstrate to the end user how online banking may be a safe banking option.

The objective of this chapter is to highlight any information identified which may shape the content of an ISA programme in the relevant literature studied. Despite the fact that the literature surveyed in this chapter is not exhaustive it is, however, sufficient to satisfy the purpose of the literature study.

2.2 Context of the Research

2.2.1 Information Security Awareness Programme

An ISA programme comprises one component of an information security management system (British Standards Institution, 2005). An ISA programme may be used to educate the end users of an information technology system on relevant threats and countermeasure available for their protection. In *NIST Special Publication 800-50*, Wilson & Nash (2003) define the important elements of an ISA programme and puts the area of focus of this research in context. According to Wilson & Nash, a security awareness and training programme is made up of four critical elements, one of which is the development of both awareness and training materials. The subject of this research study is the development of awareness materials – the content.

Figure 2-1 depicts a diagrammatic representation of these four critical elements and also of the context of this research.

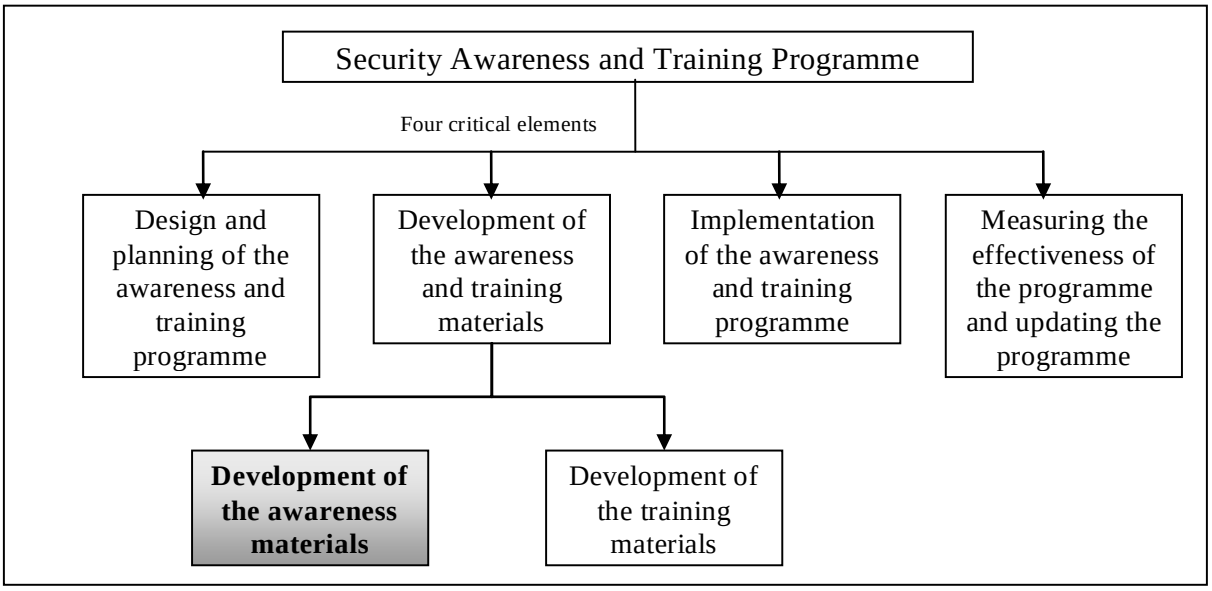


Figure 2-1 Critical elements of a security awareness and training programme

2.2.2 Home Users

The term "home users" refers to those individuals who use information technology to complete non-work related tasks outside of the workplace (ENISA, 2006). Home users may use the Internet for personal tasks such as online gaming, online shopping

and social networking. The Internet also enables home users to use online banking services.

2.2.3 Online Banking

By definition, online banking is a system which allows home users to do their banking over the Internet (Investorwords, 2011). Online banking may also be defined as a service which consumers use to conduct financial transactions in a secure manner via a website operated by their bank (Wikipedia, 2011[a]). Online banking is a convenient way in which to carry out banking tasks such as managing bank accounts, checking an account transaction history, transferring money and paying bills. Online banking eliminates the need to travel to a bank each time the customer needs to complete a transaction, thus offering the online banking users the option to bank in the comfort of their own homes. Although online banking is convenient, home users face multiple information security threats, such as phishing and social engineering, when they conduct online banking. These threats emanate from hackers attempting to obtain confidential information from home users. It is, thus, essential that the home users of online banking be made aware of both the information security threats which they face as online bankers as well as the countermeasures available to them.

2.2.4 Background to the Research

South Africans make use of both cell phone and internet banking on a daily basis. This has become increasingly evident in the South African media as major banks launch advertising campaigns promoting the benefits of these services and encouraging home users to make use of this convenient form of banking. The number of internet users in South Africa has increased from 2.4 million users in 2000 to 5.3 million users in 2009 (*South Africa Internet Usage and Marketing Report*, 2009). It is obvious that a large number of South African home users are both becoming aware of and being able to use online banking. Accordingly, from a security perspective, it is essential that the human element of the security chain be addressed (Albrechtsen, 2007; Da Veiga & Eloff, 2010; Siponen, 2001). As more functionality is added to the online banking service, so the potential for greater vulnerability increases. The public is made aware of information security incidents through media reports and notifications when logging onto the online banking service. A simple

internet search on "phishing case" will yield several results of reported phishing incidents. It is vital that these threats render banks, security professionals and home users curious about both the responsibilities of banks in this regard and also what banks are able to do to make home users aware of the information security threats they face as online bankers.

A possible solution may be the implementation of an ISA programme (Da Veiga & Eloff, 2010; Kruger & Kearney, 2008; Siponen, 2001). Such a programme would be aimed at the home users of online banking. There are best practice frameworks, such as COBIT and ISO27001, which offer ISA guidance through control objectives and controls. These frameworks are discussed further in chapter 4. Previous research (ENISA, 2006; Hansche, 2001) and publications (Desman, 2002; Wilson & Nash, 2003) offer guidance on ISA programmes. These are discussed in detail in the remainder of this chapter. It is also incumbent on banks to comply with certain laws and regulations such as the Protection of Personal Information Bill and the Electronic Communications and Transactions Act, 2002. Selected laws and regulations, which pertain to information security, are addressed in chapter 5.

An independent auditor performs an audit on an annual basis in order to verify a bank's compliance with laws and regulations such as Sarbanes-Oxley. There are other laws which recommend annual auditing although controls are investigated only should an information security incident occur, such as the Protection of Personal Information Bill. When a finding is raised, the bank is expected to remedy the finding, offer a satisfactory explanation for the finding or face legal consequences. Laws and regulations present a "do or else" scenario. In addition, banks are also service providers which rely on their customer base to remain in business. They face competition and it is essential that they keep their customers satisfied so as to prevent them from taking their business to one of these competitors. While banks need to comply with laws and regulations so as to satisfy the regulators, there is also an incentive to prevent incidents from occurring in order to maintain the confidence of their customer base.

There is a constant "cat and mouse game" between hackers and security professionals (Harris, 2008). As soon as the security professionals find a solution to counter an

attack, the hackers find new vulnerabilities to exploit and new methods for doing so. With online banking being an environment which is characterised by ever-changing information security threat vectors banks will find favour with their customers if they take a strong stance on securing the activities of home users.

In a 2010 interview conducted by Tom Field[a] with journalist and author, Joseph Menn, Menn commented on the way in which banks may gain a competitive advantage by marketing their commitment to security. In 2008, the most expensive security incidents involved financial fraud with an average loss of $500 000 per victim (Richardson, 2008). In 2009, the Anti-Phishing Working Group reported that financial services are second only to payment services (financial services were first in 2008) as the most targeted industry for phishing attacks with over 300 brands being subjected to phishing attempts in 2009. Information security threats and the consequences of breaches of security are damaging to both bank and customer. It is, thus, vitally important that banks stay abreast of the latest and most prevalent threats facing the home users of online banking and address these threats in their ISA programmes.

Chief information officers (CIOs) have considerable responsibility with regard to security incidents. If they manage to prevent an incident from being made public in the media, they normally lose the business of the customer(s) affected as well as running the risk that the customer(s) may influence the decisions of other customers on where to bank. However, if the incident does become public, the bank will suffer brand damage and loss of business. Such an incident may result from an inability on the part of the home user to identify a phishing scam and respond to it, thus resulting in identity theft. While legislation presents a "do or else" scenario, the effects of consumer ignorance present a "do or die" scenario. Without customers, a bank will not remain in business.

Although loss of business is a compelling reason to implement an effective ISA programme, nevertheless, it is essential that such a programme also be implemented in order to demonstrate due care should an incident or annual audit trigger an investigation. Due care proves that an organisation has implemented controls to protect the organisation, its resources, its employees and, in the case of online

banking, its customers (Harris, 2008). In the past, when a customer had lost money from their account, the bank would usually remedy the situation and absorb the risk itself. However, the case of PlainsCapital vs Hillary Machinery in 2010 may imply that banks are endeavouring to gain greater control over such situations.

PlainsCapital is a $4 billion bank in the United States of America and Hillary Machinery was their client. According to McGlasson (2010)[a], Hillary Machinery had $800 000 wired out of their bank account over a series of transactions. PlainsCapital managed to recover $600 000. Nevertheless, Hillary Machinery filed a lawsuit against the bank for the remaining $200 000. PlainsCaptial then filed a counter lawsuit, claiming that the incident was a result of Hillary Machinery's inadequate security measures. The case has since been settled, although details of the settlement have not been disclosed. If banks are to respond successfully, they need to satisfy due care investigations. In addition, it is essential that banks ensure all their bases are covered − one such base is that of home users. Home users are often seen as soft targets by hackers and they are targeted particularly by hackers who work for a profit. Accordingly, effective ISA programmes aimed at home users are an important component in a security plan.

The objectives of this research are to identify both the ISA requirements which legislation imposes on banks as well as the recommendations offered by information security best practices when creating an ISA programme. The researcher will perform a gap analysis to identify the differences between the legal requirements and the best practice recommendations.

2.3 Current ISA Programme Development and Assessment Instruments

Information security awareness is of utmost importance to the success of the security strategy of an organisation. According to von Solms & von Solms (2004), one of the "deadly sins" of information security is the failure to appreciate the importance of information security awareness amongst users. In this section, the available literature on ISA programme development and ISA assessment instruments is surveyed. Literature on user acceptance of online banking is included in section 2.4 to gain an

insight into users' perceptions of the online banking service. The literature on ISA programme development and assessment instruments contained in prominent electronic academic journals and databases is identified in this section. The purpose of this first part of the literature study is to investigate the guidelines for the development of ISA programme content which may be drawn from available ISA literature.

The second part of the literature study reviews factors which affect the acceptance of online banking with literature on the acceptance of online banking in prominent electronic academic journals and databases being highlighted. International studies are also included in the survey. The purpose of the second part of the literature study which identifies factors affecting the acceptance of online banking is to gain an insight into users' perceptions of the online banking service. An understanding of what prevents the end user from accepting online banking may shape the content of an ISA programme aimed at demonstrating to the end user how online banking may be a safe banking option. The researchers surveyed are in no particular order but are, instead, grouped where their work is of a similar nature. The literature surveyed is not exhaustive, nevertheless, it is sufficient to satisfy the purpose of this literature study.

2.3.1 Da Veiga & Eloff (2010)

Da Veiga & Eloff (2010) constructed a framework to create a security aware culture within an organisation. They illustrate the way in which behaviour may culminate in the prevailing culture amongst employees. Behaviour may be manipulated by the information security components which have been put in place. One such component is user security management, which includes user awareness. This framework may be adapted for home users. However, the content of an ISA programme which is aimed at an organisation's employees will not be the same as the content of an ISA programme which is aimed at online banking home users. For example, a home user's credentials provide them with access to their accounts, while a bank employee's credentials may provide them with access to the records of thousands of credit cardholders. Accordingly, the threats in these two instances are not entirely the same and, thus, the content that needs to be communicated to the two groups through an ISA programme will not be the same.

Da Veiga & Eloff identify seven information security components, with the user security management component addressing topics pertinent to a home user of online banking. These topics include trust, education and training, user awareness, ethical conduct and privacy. Da Veiga & Eloff's framework may be used to create a culture of security awareness amongst home users. For example, the bank may decide to add functionality to its online banking service. Accordingly, policies, procedures and standards – enhanced by best practices – will be either updated or compiled to address the new functionality. However, this new functionality will also create the potential for new threats. It is, thus, essential that home users be made aware of both the new functionality and how to use it in a secure manner. This involves the user security management component. Users will be encouraged to trust the application once they have been made aware of the efforts which have been made to secure it. This may include the threats they face while using the application as well as simple countermeasures which the user may implement. Requirements, as stipulated by privacy laws, must be taken into consideration and users made aware of any information as stipulated by these laws.

Da Veiga & Eloff's framework addresses threats, laws and regulations and best practice. However, the framework offers high-level, rather than case-specific, guidance as it is an all-encompassing framework, from the organisational tier to the individual tier and from board level to end user level.

2.3.2 Kruger & Kearney (2006); Kelly (2006); Wiederkehr (2003); Hansche (2001); Albrechtsen & Hovden (2009)

Kruger & Kearney (2006) developed a model for assessing the level of information security awareness in an organisation. They realised that ignorance constitutes one of the biggest threats to computer systems and that, if an ISA programme were to address this issue of ignorance effectively, it would be necessary both to measure the level of ignorance and reduce the level of it. This model by Kearney focuses on the employees of an organisation and measures three aspects: knowledge (what you know), attitude (what you think) and behaviour (what you do). These three aspects were further divided into the six focus areas which were identified in the case study which Kruger & Kearney conducted during the development of their ISA programme.

Their questionnaire aimed at testing the respondents' knowledge, attitude and behaviour in respect of the six focus areas.

Their assessment model offers a process designed to determine the content of an ISA programme. The identification of the main objectives which an ISA programme aims to realise gives the programme focus. Based both on the main objectives which have been identified and the desire to mould the knowledge, behaviour and attitude of the users so as to facilitate the realisation of these objectives it becomes possible to determine the content of the ISA programme.

Kelly (2006) also constructed a questionnaire which was designed to assess the level of security awareness within an organisation. This questionnaire was based on the most important security policies of the organisation. The objective of the questionnaire was to ensure users were aware of the most salient points contained in the most important policies. This questionnaire, like the model of Kruger & Kearney, offers a process whereby the content of an ISA programme may be determined. Kelly adopts the approach that if the security awareness amongst home users were to be evaluated, what questions would be asked? This, together with the information contained in the most important policies, forms the content of the awareness programme. However, despite the fact that this approach offers an effective starting point it does not offer specific guidance on what a South African bank should include in the content of an ISA programme aimed at the home users of its online banking service.

Like Kruger & Kearney (2006) and Hansche (2001), Wiederkehr (2003) focuses on the main objectives of the ISA programme which were defined through Wiederkehr's case study. While making use of best practices and ensuring that the latest threats are addressed, the content of the awareness programme is also based upon these objectives. The ISA programme being developed in Wiederkehr's case study is aimed at employees and, thus, makes no mention of the laws and regulations with which banks need to comply in respect of their online banking home users. However, in Hansche's list of ISA programme objectives, Hansche addresses both threats and federal laws and regulations.

Albrechtsen & Hovden (2009) use threat scenarios to shape the objectives of their ISA programme. Knowing the threats facing the home users of online banking makes it possible to construct threat scenarios. An ability on the part of home users to identify the various threats and to act accordingly constitutes the objectives of the ISA programme and moulds the content of this programme.

Based on both the literature on ISA programme objectives and an assessment of the need to secure the home users of online banking, it becomes possible to develop the content of an ISA programme. The information gleaned from the literature study does not, however, offer specific guidance in a South African context.

2.3.3 Taylor & Shepherd (2007)

Taylor & Shepherd (2007) offer guidance on awareness materials. The most notable section of their chapter is a list of eleven recommendations to be included in the ISA programme. The majority of these recommendations address threats and suggest that users be made aware of the countermeasures available that they may implement. The recommendations also address phishing, social engineering, security patches and weak passwords. However, despite the fact that these issues are all of real concern, risks are constantly changing (Kruger & Kearney, 2006; von Solms & von Solms, 2004) and it is essential that ISA programmes be kept up to date to ensure that users are aware of the latest and most prevalent threats.

Although Taylor & Shepherd offer more specific guidance on threat types, they do not address laws and regulations, nor do they suggest consulting best practice frameworks and recommendations.

2.3.4 May (2008); McKenna (2009); Siponen (2000)

Both May (2008) and McKenna (2009) offer guidance on the way in which to construct and present the ISA material but offer little on what the actual content of the ISA programme should be.

Siponen (2000) points at best practices and appropriate standards in the development of an ISA programme framework and its content. The main objective of Siponen's

article is to assess those behavioural theories which may be used in the implementation of an ISA programme in order to return a high acceptance rate by the end users. Siponen's research is useful for the implementation of an ISA programme as it attempts to present a method for persuading users to adopt the content of a security awareness programme and to alter their behaviour based on the contents of the security awareness programme. Siponen's research would probably be of assistance to banks in the implementation of their ISA programmes once the content had been compiled.

2.3.5 Desman (2002); ENISA (2006)

Desman (2002) targets professionals wanting to implement an ISA programme in an organisation. Desman is focused on building the foundation for the successful implementation of an ISA programme. This includes gaining top management approval, gathering and assessing the documentation which is already available as well as devising ways in which to facilitate smooth implementation. Such guidance would work hand in hand with a framework which was aimed at developing the content of an ISA programme and, thus, ensure smooth implementation.

The ENISA guide to raising information security awareness identifies home users as one of its target audiences. This guide offers a generic plan for creating, implementing and measuring an ISA programme. It adopts the approach of first defining the objectives of the ISA programme and then offers recommendations on how to ensure that the message reaches the correct audience. ENISA lists factors which are critical for programme success. In addition, it also stresses the importance of incorporating working lessons already learnt into the ISA programme to ensure continuous improvement. However, while comprehensive, this guide is not industry specific and it warns that a "one-size-fits-all" approach inevitably fails. Nevertheless, if this is borne in mind, the ENISA guide, like Desman (2002), would partner well with an industry specific guide on content development.

2.3.6 Kruger & Kearney (2008)

Kruger & Kearney (2008) present techniques designed to assist in deciding the most important topics to be included in an ISA programme. This is useful in preventing

information overload. Once the ISA team has compiled the potential content, these techniques could be applied to ascertain the focus areas to be addressed by the ISA programme. This offers an alternative method to identifying the objectives first and then developing the content based on these objectives. However, these techniques do not offer guidance to a South African bank in compiling the information which should be communicated to the home users of online banking.

2.3.7 Valentine (2006)

Valentine (2006) recognises the importance of industry-specific ISA programmes as opposed to a generic solution. Valentine outlines the following three phases, namely, assessment, identification and education. In the assessment phase the questions posed include: What are we protecting? What do we need to adhere to? How may we best achieve this? The identification phase asks questions such as: Who is the target audience and what threats do the members of the target audience face? What do they need to know? The education phase deals with training and is, thus, outside of the scope of this research. Valentine's article would be of assistance to the ISA team in kick-starting their thinking about the objectives of the ISA programme although it does not offer specific guidance for ensuring that all the relevant content is considered.

2.3.8 Siponen (2001)

The number of home users who are potential targets for hackers is increasing constantly. As a result, Siponen (2001) has identified the need to extend information security awareness beyond the borders of an organisation into the public domain. Siponen identifies five dimensions of information security awareness. These five dimensions address the following:

- insider threats in the organisational dimension
- latest and most prevalent threats in the general public dimension
- laws and regulations in the sociopolitical dimension
- the connection between security and ethics in the computer ethical dimension
- the need for education to alter the behaviour of users in an attempt to mitigate the risks facing them

These dimensions offer useful guidance on those issues that an ISA programme should address. However, there is still no industry-specific guidance available.

2.3.9 Rotvold (2008)

Rotvold (2008) focuses on ISA programmes which are aimed at the employees of an organisation. Rotvold encourages the ISA team to identify the major objectives of the ISA programme and to communicate these objectives to create a security culture. The paper offers a helpful list of topics for inclusion in an ISA programme – these topics include threats, countermeasures and compliance with laws and regulations. However, when using this document as a guideline it is essential that, the ISA team or security officer remain cognisant of the fact that these topics are not necessarily all relevant to the home users of online baking.

2.3.10 Peltier (2005)

According to Peltier (2005), an organisation may have the best security measures in place but, if the end users are not aware of the dangers they face, the security plan will not succeed. In common with the warnings of the ENISA guide, Peltier highlights the importance of making the content of an ISA programme relevant to the target audience. Peltier goes on to recommend that the ISA team conduct a risk assessment which should be supplemented by an analysis of the breaches reported in the media involving home users. A risk assessment is a good starting point in the compilation of an ISA programme. In addition, it is vital that the ISA team ensure that risks associated with non-compliance with laws and regulations are included in the risk assessment. Where relevant, best practices should also be taken into account when compiling the content for the ISA programme.

2.3.11 Wiles, Claypoole, Henry, Drake & Lowther (2008)

Wiles, Claypoole, Henry, Drake & Lowther (2008) include a chapter on developing an effective security awareness programme where customers are included in the target audience. However, despite the fact that Wiles et al also address the issues of privacy and compliance and stresses the importance of these issues, the guidance given by them is high-level and not specific to the case of South African home users of online

banking. Wiles et al also cover categories of awareness evaluation which may, in turn, be interpreted as the threats facing home users. Like Desman (2002) and Taylor & Shepherd (2007), the objective of the chapter by Wiles et al is to offer high-level, generic guidance for an ISA programme.

2.4 Acceptance of Online Banking

An identification of factors affecting the acceptance of online banking is helpful for gaining an insight into users' perceptions of online banking services. In addition, an understanding of what prevents the end user from accepting online banking will enable the ISA team, through the ISA programme, to demonstrate to the end user how online banking is a safe banking option.

In this section, a number of acceptance studies will be analysed to determine factors that prevent users from accepting online banking. It is hoped that this will point to the need for certain content to be included in an ISA programme.

Al-Somali et al (2009) identified trust as a factor affecting the acceptance of online banking. Users place high importance on being able to trust their online transactions and are more willing to commit to using an online service if they feel they are able to trust the service. Al-Somali et al (2009) found that, if banks demonstrated the safety features of online banking, users would be encouraged to use the service.

Sathye (1999) found that 77% of personal respondents who were aware of online banking and 95% of personal respondents who were not aware of online banking cited security concerns as a factor affecting their acceptance of online banking. These percentages constitute a high percentage of potential business. An ISA programme could, thus, highlight the security measures taken by a bank in the case of online banking so that, as users become aware of the online banking service, they would also become aware that the service is safe to use. In addition, the ISA programme should also communicate the roles and responsibilities of the users in making online banking a safe service to use.

Kim, Tao, Shin and Kim (2010) recognise that, if users believe online banking is safe, they will trust the service and this will, in turn, lead to increased acceptance of the service. Kim et al focus on e-payment systems such as e-cash, and debit and credit cards. While this does not refer specifically to online banking, the concepts are similar with similar risks. The findings of this research emphasise the need for advertising the good security measures associated with the service to nurture trust.

Sadique Sohail & Shanmugham (2003) identify trust and security concerns as two major factors affecting acceptance of online banking.

It would appear there is sufficient support for banks to advertise their stance on security. An appropriate vehicle for this would be their ISA programmes, in which the banks encourage users to make use of the online banking service. However, Pikkarainen et al (2004) also tested security and privacy as possible deterrents to the acceptance of online banking. They found that there is, in fact, a weak link between security and trust and the acceptance of online banking. However, despite this finding, these studies encourage ISA teams to promote the banks' stand on security as well as the role of users in making online banking a safe service. In this way banks are also able to demonstrate to potential abusers that they are serious about security and will enforce consequences should a breach occur (Blumstein, 1978).

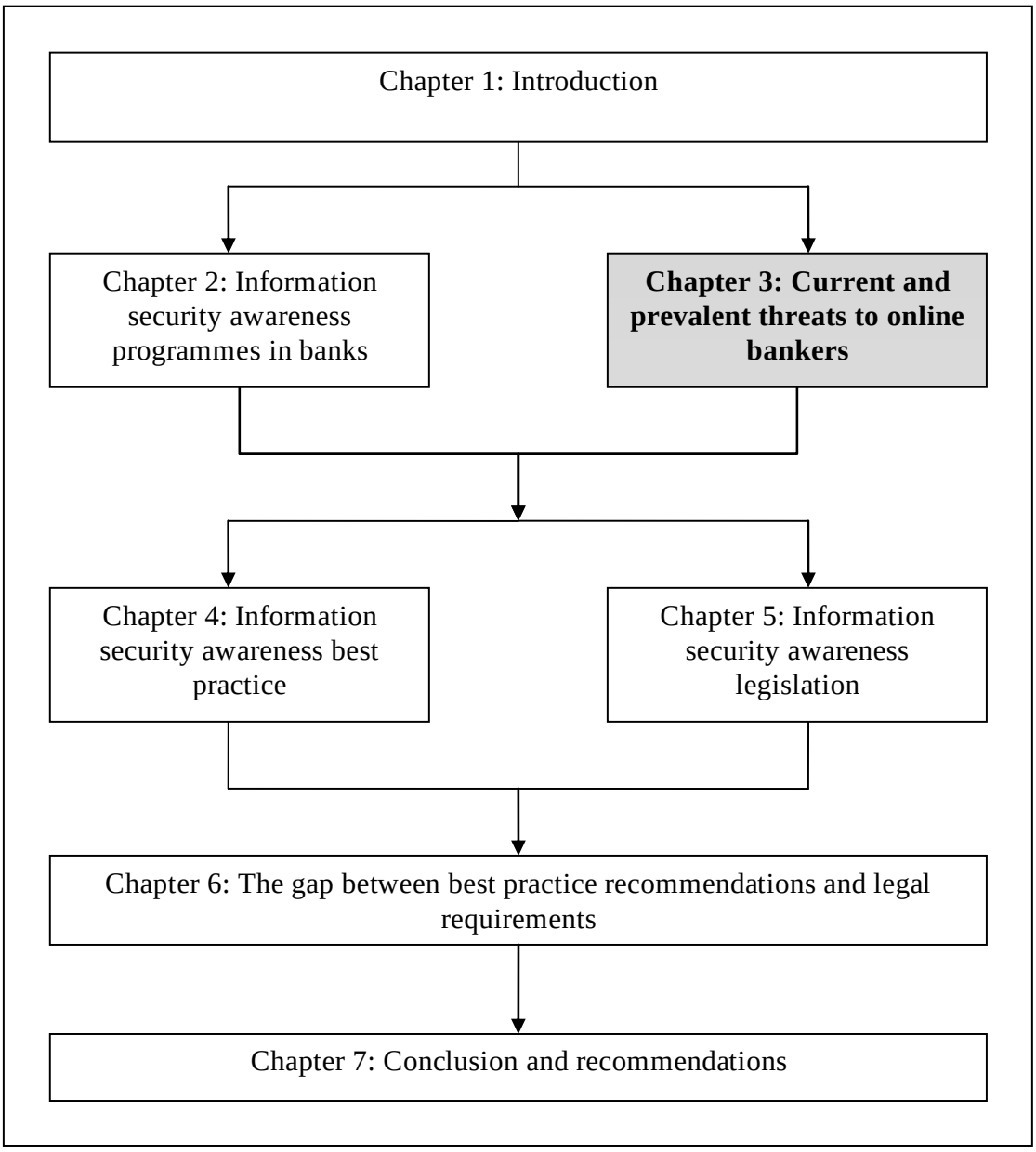
2.5 Summary

The literature surveyed addresses information security awareness within organisations as well as awareness initiatives aimed specifically at home users. A significant portion of the literature surveyed is of a generic nature, thus highlighting the need for more industry-specific, even case-specific, guidance. Although rarely found in the same research, results from this literature survey indicate that there are three major dimensions that should be taken into account when creating an ISA programme. These dimensions include, firstly, information security threats to online bankers; secondly, laws and regulations or the need for banks to comply with legislation; and, thirdly, the use of best practice. Information security threats create the need for legislation to regulate the banking industry as well as motivating the need for information security initiatives, such as ISA programmes, to be implemented. Based

on the results of the literature survey in this chapter, this research study aims to identify both the requirements imposed on banks by laws and regulations as well as the recommendations made by information security best practice when creating the content for an ISA programme aimed at the home users of online banking. These are compared to determine whether the implementation of best practice recommendations will result in compliance with the requirements as stipulated by the relevant laws and regulations.

Chapter 3:

Current and Prevalent Threats to Online Bankers


Chapter 1: Introduction
Chapter 2: Information security awareness programmes in banks
Chapter 3: Current and prevalent threats to online bankers
Chapter 4: Information security awareness best practice
Chapter 5: Information security awareness legislation
Chapter 6: The gap between best practice recommendations and legal requirements
Chapter 7: Conclusion and recommendations

3.1 Introduction

Online banking offers home users with access to the Internet a convenient way to complete personal banking tasks such as checking account balances, transferring money and paying accounts. However, as the end users of the online banking service, home users also face multiple information security threats. These information security threats include social engineering, phishing and the installation of malware (Furnell, 2008; Granova & Eloff, 2005). Recently, hackers have been using a blend of these threats when attacking their targets. For example, a phishing scam may tempt a user to click on a link which automatically downloads malware onto the home user's personal computer. This malware may have the ability to monitor keystrokes and, thus, send information about the home user's banking accounts to the hacker. It is, therefore, imperative that banks make their customers aware of both information security threats as well as simple countermeasures they may implement. Banks are able to achieve this through an Information Security Awareness (ISA) programme. Nevertheless, the methods used by hackers are constantly evolving, thus requiring that the information communicated to the home user be kept current.

The objective of this chapter is to investigate the latest and most prevalent information security threats facing the home users of online banking. These threats have created the need for legislation aimed both at regulating information security in the banking industry and at motivating the need for the implementation of information security initiatives such as an ISA programme. Selected electronic sources will be analysed for information on information security threats. In addition, this chapter explains the way in which these documents were selected and how the documents were analysed. The culmination of this chapter is a top 10 list of the information security threats facing the home users of online banking. Throughout this chapter, information security threat terms are used. These terms are defined in Table 3-1.

Table 3-1 Information security threat terminology

Term	Definition
Phishing	Phishing is an illegal attempt to obtain confidential and sensitive information either by email or by acting as a trusted party (*Oxford English Dictionary*, 2011[b]; Wikipedia, 2011[c])
Social engineering	Social engineering is the act of convincing a person to reveal confidential and sensitive information by acting as a party authorised to obtain that information (Harris, 2008; Wikipedia, 2011[d])
Malware	Malware is an abbreviation for malicious software and refers to code written to access a system in an unauthorised manner. Examples include viruses, worms and trojans (Harris, 2008; Wikipedia, 2011[e])
Encryption	In cryptography, encryption is the process of transforming information in its readable form to an unreadable, encrypted form (Harris, 2008; Wikipedia, 2011[f])
Authenticate	Authentication is used to validate the identity and access rights of a subject when requesting access to an object, for example a home user's attempt to access the online banking service (Harris, 2008)
Firewall	A firewall is a network component used to block and allow communication into and out of the network, based on configured rules (Wikipedia, 2011[g])
Spoofing	Spoofing is used to describe a method of attack where the attacker acts as a trusted party, such as phishing, by hiding the origin of the message (Harris, 2008)
Antivirus	Antivirus software is used to prevent malware installation, detection of installed malware, and remove installed malware (Wikipedia, 2011[h])
Identity theft	Identity theft refers to fraud committed by a party acting as another party authorised to receive benefits, such as money (Wikipedia, 2011[i])

3.2 Documents to be Analysed

The objective of the analysis of selected documents is to create a "Top 10" list of the threats facing the home users of online banking. These threats are then matched with countermeasures that the home user may implement. For example, the user's connection to the bank's mainframe may use an SSL link although this does not protect the user's computer. It is the responsibility of users to install personal firewalls and to ensure that the antivirus software on their computers is switched on and up to date. These threats facing the home users of online banking drive the need both for legislation aimed at regulating the banking industry and the implementation of ISA initiatives to educate home users on how to protect themselves.

ISA programmes should address those threats which are current and pertinent. Accordingly, the sources used to identify these threats should have the following attributes:

- an information security focus
- published content, written in the last two years, on current security topics
- include, in their reporting, security threats which would target the home users of online banking

The documents for analysis were taken from both electronic sources and electronic academic journals characterised by the above attributes. These documents were analysed for both information security threats facing online bankers as well as security countermeasures. The findings list the threats facing the home users of online banking as identified in the selected documentation. However, it would not be possible to include each attack type in an ISA programme as this may lead to an information overload. Accordingly, this chapter ultimately proposes a top 10 list of the information security threats facing home users of online banking which should be addressed by an ISA programme.

The following electronic sources were identified:

- SANS (www.sans.org)
- National Cyber Security Alliance (www.staysafeonline.org)
- CSOOnline (www.csoonline.com)
- CIO (www.cio.com)
- Bankinfosecurity (www.bankinfosecurity.com)
- Elsevier academic papers (accessed online via UNISA Library)

Although this is not an exhaustive list, for the scope of this research these sources may be considered sufficient.

The electronic sources are analysed as follows:

- SANS.org was surveyed for the SANS Security Tip of the Day. These tips were categorised into the types of attacks which they address and the relevant attacks were added to the SANS list.
- The National Cyber Security Alliance's (NCSA) 2010 National Cybersecurity Awareness Month's document, entitled *What Home Users Can Do,* was analysed for the information security threats facing home users. The NCSA website (www.staysafeonline.org) was also consulted for countermeasures which are available for home users to implement.
- CSOonline.com and CIO.com were analysed for recent security articles addressing the information security threats facing the home users of online banking.
- Bankinfosecurity.com was surveyed for the latest information security breach reports involving financial institutions and for articles addressing the information security threats facing home users. Cybercrimes targeting the home users of online banking were also pinpointed.
- Elsevier academic papers were searched for articles published in the last two years on threats facing online bankers.

In addition, it is suggested that banks should also research their own records to extract recent incidents involving their home users of online banking. This would give them some insight into what their customers need to be protected from.

3.3 Narrowing the list to a "Top 10"

It is, however, not possible to include each information security threat in the ISA programme as this may lead to an information overload when communicating threats and countermeasures to the home user. Accordingly, the results of the document analysis were scaled down to represent a final top ten.

Within an organisation it is recommended that a risk assessment type approach be adopted to narrow down the list of threats. A risk may be defined as the probability that a threat exploits a vulnerability, resulting in damage to the business (Harris, 2008). Each threat would need to be rated on the probability of it occurring and the potential damage, should it occur. This would need to be deliberated by a specially

selected group representing top management, middle management as well as technical staff. The group should also include representatives from outside of IT from, for example, finance, marketing and human resources. A limitation to this research is that the research will not demonstrate this process.

3.4 Building the Threat List

In this section, each website and magazine is briefly described and the method used to survey the source explained. Thereafter, a table is presented displaying the threats facing the home users of online banking, any countermeasures specified by the source and the source's reference. In conclusion, a summary of the threats is displayed in a further table.

3.4.1 SANS

The SANS (System Administration, Audit, Network, Security) Institute was established in 1989 and is active in both research and educational activities. Currently, SANS is a leading global provider of information security training and security certification. SANS reaches over 165 000 security professionals who contribute to the information security repository. SANS also makes freely available the largest collection of information security research documents in the world. SANS has been cited by numerous articles, mostly for its certifications and standards. These articles include:

- "Information Security Policy – what do information security standards say?", (Höne & Eloff, 2002)
- "Why we need a new definition of Information Security" (Anderson, 2003)
- "Wired versus Wireless Security: the Internet, WAP and iMode for E-Commerce" (Ashley, Hinton, Vandenwauver & IBM Software Group, 2001)

Resources available on SANS.org include:

- security tip of the day
- a weekly news digest

- a weekly vulnerability digest
- over 1 200 award-winning information security research papers

For this research study, the SANS Tip of the Day content was analysed for the threats which each tip addresses. The SANS Tip of the Day content is focused on security and addresses current threats. It also includes those threats affecting the home users of online banking.

The SANS Tip of the Day was collected for the preceding four months − May 2010 to August 2010. Attacks relevant to home users of online banking are presented in Table 3-2.

Table 3-2 SANS Threats

Tip	Threat(s) Identified	Countermeasure (if specified)
Check for encryption or secure sites when providing confidential information	Minimal protection for confidential data	
Use Google's cached mode to avoid spyware	Keystroke logging to capture online banking authentication credentials	
Be sceptical when you read your email	Phishing, social engineering	
Wireless hotspots. Limit activity to web surfing only	Minimal protection for confidential data	Use a good personal firewall and ensure software patches are up to date. Never do online banking at public hot spots.
Watch out for shoulder surfers	Shoulder surfing to gain online banking authentication credentials	Ensure no-one is watching over your shoulder when you input your online banking credentials.
Keep your password secret	Unauthorised access to your online banking account	Keep your password a secret to prevent others from abusing your account. If you share your password, your bank may not refund you stolen funds.
Email is not the only online communication that has security risks	Installation of malware to capture online banking authentication credentials	Understand the security risks associated with online communication such as Instant Messaging. Hackers are able to transfer malware which may log your keystrokes when you are logging into your online banking account.
Do not install Microsoft updates and patches sent by email (They are fake)	Installation of malware to capture online banking authentication credentials	Hackers are able to transfer malware which is able to log your keystrokes when you are logging into your online banking account.

Tip	Threat(s) Identified	Countermeasure (if specified)
Do not fall for phishing schemes	Phishing	Avoid emails from "your bank" containing the following phrases: • We need to verify your account information • If you do not respond immediately, your account will be cancelled • Click the link below to update your information
Change your password on a schedule	Password guessing	Keep passwords complex and change them periodically to better protect your online banking account.
When you logout, logout completely	Misuse of your online account by another person	Logout completely when you have finished your online banking and do not set your browser to remember your password.
Ten scams to screen from your email	Phishing, spoofed websites	• The "Nigerian" Email Scam • Phishing • Work-at-Home Scams • Fake software updates • Foreign lotteries • Sexual enhancement products • Check overpayment scams • Pay-in-Advance credit offers • Debt relief • SARS funds
Do not click on links in pop-ups or banner advertisements	Phishing, keystroke logging	Right click on the banner or pop-ups window on the task bar and click on Close.
Beware of a USB flash drive's autoplay feature	Installation of malware from an unknown USB	Disable the autoplay feature in the drive's properties.

Tip	Threat(s) Identified	Countermeasure (if specified)
If your browser questions a websites security, stop, think and verify	Spoofed or compromised website	Do not ignore warnings such as "There is a problem with the website's security certificate" or "Secure Connection Failed". Contact your bank by telephone and query the warning before proceeding.
Use a password in one place only	Password capture or guessing	Do not use your online banking password for other accounts. The databases at other companies may not be as well protected, thus enabling hackers to obtain your online banking password.
Stop! Nobody sends email to dead people!	Phishing	Do not respond to phishing emails asking you to verify that you are alive by sending personal and financial information.
It takes two to tango and two firewalls to secure your system	Hacking and installation of malware	If you have a home network, install both a hardware firewall and a software firewall on each connected computer.
Do not trust links sent in email messages	Phishing	Ignore these emails as banks do not send emails requesting personal or financial information.
Do not download files from unknown sources	Downloading of malware	If you are uncertain, do not download files from unknown sources.
Do not plug in USB drives that you find lying around. Criminals may use them to steal your data.	Loading of malware	Malware may be loaded, enabling hackers to steal your information or take control of your computer
Delete files effectively	Capture of personal and financial information	Do not leave documents containing sensitive information in your Recycle Bin. Empty the trash.
If you access the Internet from a shared computer, make sure you do not leave anything behind	Unauthorised access to your online banking account	• Do not check the "Remember my password" box • Log off completely • If possible, clear both the browser cache and history • Never leave the computer unattended while you are logged in • Delete all documents you have used and empty the recycle bin

Tip	Threat(s) Identified	Countermeasure (if specified)
Look before you click	Phishing, spoofed websites, download of malware	Do not open emails if you are unable to ascertain who the sender is.
Do not allow Internet Explorer to store passwords for you	Unauthorised access to your online banking account	Ensure that the box for Internet Explorer to remember your password is unchecked, particularly on shared computers.
Four tips to keep your computer secure	Download of malware	Install the following: • Antivirus • Anti-spyware • Two way personal firewall • Anti-keylogger
Do not use information related to yourself as a password	Password guessing	
Patch and update on a regular basis	Hacker exploitation of vulnerabilities to gather information off your computer or to take control of your computer	
Make your password long	Password guessing	Try entering a passphrase. If it is not allowed, choose a password longer than 8 alphanumeric (letters and numbers) characters.
Do not use unauthorised software	Downloading of malware, such as spyware, to obtain your confidential information	

3.4.2 National Cyber Security Alliance

The National Cyber Security Alliance (NCSA) forms strategic public and private partnerships with the intention of building and implementing education and awareness efforts aimed at home users, employees and students. The information disseminated through these efforts equips users with the knowledge and tools they need to keep themselves, their organisations, their systems, and their sensitive information safe and secure online, thus encouraging a security aware culture. The NCSA's efforts in 2009 reached over 40 000 000 people worldwide.

The NCSA released a document for their National Cybersecurity Awareness Month entitled *What Home Users Can Do*. The awareness month was October 2010. This document is current and addresses current threats. It also includes threats to the home users of online banking. The NCSA has been cited by numerous articles, most of which focus on home user security and security awareness. The articles include:

- "Why users cannot use security" (Furnell, 2005)
- "The psychology of security" (West, 2008)
- "Unrealistic optimism in Internet events" (Campbell, Greenauer, Macaluso & End, 2007)

This document was reviewed for the threats as addressed by their tips for home user online safety. Table 3-3 presents the threats related to the home users of online banking.

Table 3-3 NCSA Threats

Threat Identified	Countermeasure (if specified)
Installation and downloading of malware which may allow hackers to monitor keystrokes, obtain confidential information from your computer or take control of your computer	Use a set of security tools including anti-spyware, antivirus and personal firewalls.
Vulnerabilities in software which hackers may exploit	Make sure your operating system, web browser and other software is updated.
Password guessing, resulting in unauthorised access to your online banking account	Use long, complicated passwords or passphrases made up of alphanumeric characters. Change passwords periodically.
Falling victim to phishing scams or spoofed sites and giving away confidential personal and financial information	Stay alert and be careful not to give out confidential personal and financial information.
Working on an infected computer	Be aware of slower processing times, pop-ups and other unusual activities on your computer.
If your home computer is shared, the other users may be unaware of security risks and perform activities which put both your computer and your information at risk. For example, checking the "Remember Password" box on Internet Explorer	Educate family members and other users of your home computer on security risks and countermeasures.

3.4.3 CSOOnline

CSO provides news, analysis and research and focuses on information security, physical security, business continuity, identity and access management and loss prevention. CSO is produced by CXO Media which is an award-winning member of the International Data Group. CXO Media also produces CIO.com. The CSO content is current and includes, in its reporting, threats facing the home users of online banking. CSOOnline articles have been cited during presentations at information security conferences. These articles include:

- "High time for trusted computing" (Potter, 2009)
- "A framework for reasoning about the human in the loop" (Cranor, 2008)
- "Information security: an organisational change perspective" (Cline & Jensen, 2004)

The CSO website was searched using the following search terms:

- top threats online bank
- online bank threats home user
- security awareness home user

The searches yielded several relevant articles. These articles were then analysed for threats facing the home users of online banking. Table 3-4 presents the threats related to the home users of online banking.

Table 3-4 CSOOnline threats

Threat Identified	Countermeasure	Reference
Social engineering	Identify the attack, end communication and report the incident.	Goodchild, 2010[a]
Phishing	Identify the attack, do not respond or click on any links, and report the incident.	Goodchild, 2010[b]

3.4.4 CIO

CIO.com's target audience includes chief information officers and other IT leaders. CIO was established in 1987 and kicked off with CIO magazine. CIO provides technology and business leaders valuable analyses of both IT trends and the role of IT in realising business goals. Both the magazine and the website have received more than 160 awards. CIO content includes security topics and reports on threats facing the home users of online banking. CIO.com articles have been cited by other articles focusing mainly on IT as a business enabler. These articles include:

- "The evolution of the KM function" (Smith & McKeen, 2003)
- "Synergizing the learning organisation and knowledge management" (Loermans, 2002)
- "An overview of IT service management" (Galup, Dattero, Quan & Conger, 2009)

The CIO website was searched using the following search terms:

- Online banking threats home users
- Top threats
- Phishing

The searches yielded several relevant articles published in the last two years. These articles were analysed for threats facing the home users of online banking. Table 3-5 presents the threats related to the home users of online banking.

Table 3-5 CIO Threats

Threat Identified	Countermeasure (if specified)	Reference
Phishing	Identify the attack and do not respond.	McMillan, 2009
Phishing	Use anti-spyware software and do not post personal information on social networking sites.	Dahdah, 2008
Cross-site scripting (XSS)	Install trusted software designed to alert you when you are redirected from a legitimate site to a spoofed site.	Spring, 2007
Malware – emails containing malware that collects confidential personal and financial information	Install antivirus software and keep it up to date.	Hwang, 2008
Phishing	Be suspicious of emails and websites requesting or requiring confidential personal and financial information.	Hwang, 2008
Malware – installing software or services from an distrusted company	Use only products from trusted companies and obtained via legitimate channels.	Hwang, 2008
Links in greeting emails – these may install malware	Do not click on these links.	Hwang, 2008
Trojan intercepts online banking transactions and changes the destination account's details to a hacker's account details		Weil, 2008

3.4.5 Bankinfosecurity

BankInfoSecurity is published by the Information Security Media Group, Corp. (ISMG) and specialises in information security, risk management and fraud. BankInfoSecurity.com provides reliable and current information on information security in financial institutions. The website addresses both dynamic compliance mandates and information security incidents such as breaches and other fraudulent activities.

The articles are contributed and reviewed by a number of accomplished individuals, including risk management practitioners, industry experts and technology providers. These articles include reports on threats facing the home users of online banking. BankInfoSecurity.com articles have often been cited, mostly in articles dealing with data security in financial institutions. These articles include:

- "Warranting data security" (Moringiello, 2010)
- "Security issues in banking systems" (Ahmad, Rosalim, Yu Beng & Soo Fun, 2010)
- "ATM risk management and controls" (Rasiah, 2010)

The Bankinfosecurity website was searched using the following search terms:

- security breaches
- home users
- online threats

The searches yielded several relevant articles. These articles were analysed for threats facing the home users of online banking. Table 3-6 presents the threats related to the home users of online banking.

Table 3-6 BankInfoSecurity Threats

Threat Identified	Countermeasure (if specified)	Reference
Exposure of data on the Internet	Google your name, address and identity number periodically and report the incident if found	McGlasson, 2010[b]
Phishing, spoofed websites	Learn to identify a potential phishing email or website, for example, check spelling and grammar. Be sceptical about emails and websites asking for confidential personal and financial information. Contact your bank telephonically to verify the validity of the request.	Dhamija, Tygar & Hearst, 2006
Password guessing	Strong password characters.	RSA, 2007
Phishing	Educate consumers and encourage them to educate themselves on identifying a phishing email or website.	RSA, 2007
Phishing, identity theft	Implementation and enforcement of strong authentication methods by the bank	VeriSign, 2008
SARS phishing email	Identify the attack, do not respond and report it	VeriSign, 2007
Malware		VeriSign, 2007
Malware	Make use of antivirus software and personal firewalls. Ensure these are kept up to date. Be sceptical of links and attachments in emails.	Field, 2010[b]
Phishing, identity theft	Implementation and enforcement of strong authentication methods by the bank.	SafeNet, 2009
Phishing		Symantec, 2007
Malware		Symantec, 2007
Malware	Use antivirus software. Make sure all patches and software are up to date. Be wary of email attachments and links.	Donchez, 2008
Phishing	Beware of emails from banks, eBay, SARS or other sites prompting you to upgrade your information. Do not click on links in the email to the relevant institution's site.	Donchez, 2008
Password guessing	Use a long, alphanumeric password. Really secure passwords are over 15 characters long.	Donchez, 2008
Phishing		Swart, 2007

Threat Identified	Countermeasure (if specified)	Reference
Malware that captures keystrokes and credentials		Swart, 2007
Malware		Field, 2009
Phishing, social engineering and identity theft		SafeNet, 2010
Credential gathering malware		SafeNet, 2010
Man-in-the-Browser (MITB) Attack	Use antivirus software and keep this software updated. Take precautions not to download or accidentally install malware.	SafeNet, 2010
Identity theft	Implementation and enforcement of strong authentication methods by the bank.	SafeNet, 2010

3.4.6 Elsevier Academic Papers

Elsevier is the world's largest scientific, technical and medical information provider and forms part of the Reed Elsevier plc group, a world-leading publisher and information provider. Elsevier publishes academic papers which address information security topics, such as threats facing the home users of online banking.

Elsevier articles were searched using the following search terms:

- threats home users
- threats online banking
- home user security

For the purposes of this research, articles published during the last two years and which addressed threats facing the home users of online banking were analysed.
Table 3-7 presents the threats related to the home users of online banking as extracted from these articles.

Table 3-7 Elsevier threats

Threat Identified	Countermeasure (if specified)	Reference
Phishing	Alias email address, digitally signed emails	Bose & Leung, 2008
Malware	Make use of and keep updated antivirus, anti-keylogging and anti-trojan software as well as a personal firewall.	Bose & Leung, 2008
Spoofed sites	Digital server certificate, trusted path ensured browser	Bose & Leung, 2008
Identity theft	Two-factor authentication, zero knowledge proof	Bose & Leung, 2008
Malware		Brenner, 2007
Fraud (phishing)		Brenner, 2007
Phishing		Dodge, Carver & Ferguson, 2007
Social engineering		Dodge et al, 2007
Malware		Dodge et al, 2007
Phishing		Furnell, Tsaganidi & Phippen, 2008
Malware		Furnell et al, 2008

3.5 The Top 10 List

The major threats facing home users which were identified were those threats which aided identity theft. The threats most frequently identified included phishing, spoofed or compromised websites and malware. Identity theft occurs once the perpetrator has obtained confidential information, such as online banking authentication credentials, through attack methods, such as phishing and social engineering, and then proceeds to impersonate the victim at a particular organisation's website, such as a banking website. Table 3-8 presents a summary of the threats that were identified as well as those sources which identified the threat. Despite the fact that identity theft is mentioned infrequently, it may be assumed that identity theft is, indeed, the intention of the perpetrator who is endeavouring to acquire the confidential information.

To avoid information overload, the number of threats addressed by an ISA programme should be limited to a top 10. For the purpose of this research, the threat list was narrowed down to include those threats which were mentioned by the greatest number of sources. Of the 15 threats identified, seven were cited by one source only. Of these seven threats, the two threats most often identified by the source included the existence of sensitive files in the user's recycle bin and minimal protection afforded to confidential data during online transactions. These threats were mentioned twice each by SANS.org. The remaining five threats were all mentioned by their sources only once. The top 10 threats are

- phishing
- spoofed websites
- keystroke logging
- malware
- social engineering
- minimal protection afforded to data
- password guessing or password theft
- sensitive information in the user's recycle bin
- shared computer threats
- out of date patches and software

Table 3-8 Threat summary

	SOURCE					
THREAT	SANS	NCSA	CSOOnline	CIO	BankInfoSecurity	Elsevier
Phishing, spoofed sites	✓	✓	✓	✓	✓	✓
Keystroke logging	✓	✓			✓	
Malware	✓	✓		✓	✓	✓
Social engineering	✓		✓			✓
Minimal protection afforded to confidential data	✓					
Shoulder surfing	✓					
Password guessing or theft	✓	✓			✓	
Misuse of your online account by another person	✓					
Sensitive info in recycle bin	✓					
Shared computer threats	✓	✓				
Out of date patches and software	✓	✓				
Cross-site scripting				✓		
Exposure of personal data on the Internet					✓	
Man-in-the-Browser attack					✓	
Identity theft					✓	✓

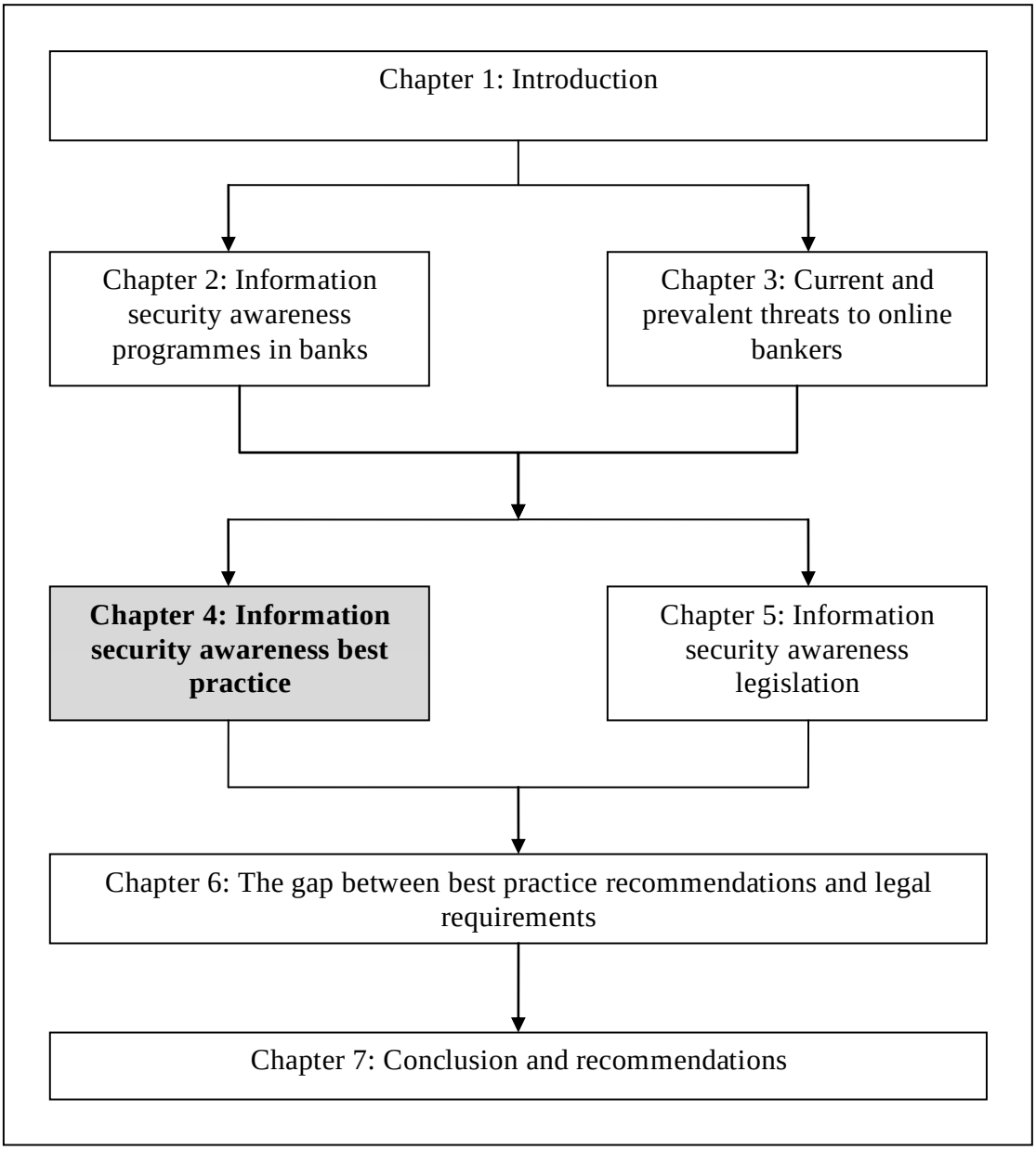
3.6 Summary

In this chapter, the most prevalent threats to online bankers were identified. These threats drive both the need for legislation aimed at regulating the banking industry and the need to implement an ISA programme designed to educate home users on how to protect themselves when banking online. It was found that aided identity theft was the most common threat. Despite the fact that other threats exist which may have a bearing on the content of an ISA programme, these threats were identified by the sources selected for this research.

In the next two chapters, selected best practices will be analysed for recommendations when implementing ISA programmes and selected laws and regulations will be analysed for the requirements imposed on banks when implementing ISA programmes aimed at the home users of online banking.

Chapter 4:

Information Security Awareness Best Practice


Chapter 1: Introduction
Chapter 2: Information security awareness programmes in banks
Chapter 3: Current and prevalent threats to online bankers
Chapter 4: Information security awareness best practice
Chapter 5: Information security awareness legislation
Chapter 6: The gap between best practice recommendations and legal requirements
Chapter 7: Conclusion and recommendations

4.1 Introduction

In industry, organisations attempt to outdo their competitors and gain a competitive edge by providing a better service or product than their rivals. The methods and procedures adopted to provide services or manufacture products are constantly reviewed and improved over time in an effort to find an optimal way of doing things. Those methods and procedures which were considered at the time to produce the most desirable outcome become known as industry best practice. A best practice may be defined as a procedure or method which is known to achieve the best possible results (BusinessDictionary, 2011; Methods & Tools QA Resources, 2009; Wikipedia, 2010[b]). In this chapter, the focus is on information security best practices and international standards. Information security best practices and international standards are important for effective information security governance (von Solms & von Solms, 2004). Banking organisations implement best practices for a number of reasons which include improving customer confidence in the banks' security programmes and ensuring that their information security programmes are at a standard where, should a security breach occur, the bank concerned will be able to demonstrate due care and due diligence and, thus, avoid financial and legal consequences (von Solms & von Solms, 2004; Williams, 2008).

This chapter will investigate the recommendations proffered by internationally recognised information security best practices or standards to organisations in respect of user awareness. In addition, the criteria for the selection of these best practices or international standards will be defined.

4.2 Documents to be Analysed

The objective of the analysis is to compile a list of recommendations which organisations could implement when striving to comply with international information security best practices. This chapter discusses the background to each best practice selected, the objective of the best practice and its structure. User awareness recommendations are extracted from each best practice and interpreted in a way which may be relevant to an information security awareness (ISA) programme aimed at the home users of online banking.

The criteria for the selection of the best practices to be included in this research include the following:

- it must be an internationally accepted information or information security standard which may be implemented in a banking organisation.
- it must be available to the public.

For each selected best practice, recommendations relevant to user awareness are extracted and interpreted in the context of an ISA programme aimed at the home users of online banking. These recommendations are presented in tables specific to each selected best practice.

The best practices or international standards identified include the following:

- COBIT (Version 4.1)
- ISO/IEC 27001
- Standard of Good Practice for Information Security (2007)

Despite the fact that this list is not exhaustive the sources are considered sufficient for the purposes of this research.

4.3 Compiling the Best Practice Recommendations List

In this section, each best practice selected is introduced and its background described. Thereafter, a table is presented which displays the recommendations identified that banks should adopt in their endeavours to comply with the selected best practice. These recommendations are interpreted in the context of an ISA programme aimed at the home users of online banking. All the tables are then consolidated into one "recommendations" table. This latter table lists the best practice recommendations and the corresponding best practice control references, thus facilitating the identification of which international standard covers which recommendation. Finally,

a table listing the best practice recommendations only is presented. This table constitutes the best practice recommendations list.

4.3.1 COBIT 4.1

COBIT 4.1 was an incremental update to COBIT 4.0 and was released in 2007. It was also preceded by COBIT 3rd Edition, published in July 2000. COBIT is an acronym for Control Objectives for Information and related Technology. The mission of COBIT is to create a current, international IT governance control framework which is publicly available for use in organisations. Business managers of organisations and IT and assurance professionals comprise the target audience for this standard. COBIT adopts a process-oriented approach with control objectives defined for each process. There are 34 processes grouped in the four COBIT domains. These domains include Plan and Organise, Acquire and Implement, Deliver and Support, and Monitor and Evaluate. However, not all processes necessarily apply to one single organisation. Although COBIT 4.1 also offers guidance on aspects such as assigning accountability and performance metrics this research study will only go as far as the control requirements. COBIT presents the control objectives an organisation should satisfy rather than the steps an organisation can take to satisfy these control objectives. It is up to the organisation to identify its needs, select relevant COBIT processes and implement controls in a manner that will be effective in the organisation concerned and also meet the control objectives.

COBIT is applicable to all organisations − worldwide − which require and/or implement IT controls. A history of COBIT implementations lists multiple industries around the globe which have implemented COBIT (Ridley, Young & Carroll, 2004). It is suggested that an organisation refer to COBIT should the organisation need to align its IT with its business objectives. COBIT has been referred to in numerous published articles, in particular, articles addressing information and information technology governance and control. These articles include:

- "COBIT: a methodology for managing and controlling information and information technology risks and vulnerabilities" (Lainhart, 2000)

- "IT governance hands-on: using COBIT to implement IT governance" (Kordel, 2004)
- "Information security governance: COBIT or ISO 17799 or both?" (von Solms, 2005)
- "Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges" (Hardy, 2006)

COBIT may be used to mould the entire security posture of an organisation. However, for the purpose of this research, the focus will be on the security process which deals specifically with end user training and education. Attention will also be paid to related COBIT processes which act as inputs to this process. Control objectives will be analysed and interpreted in the context of this research under the "Applicability" column. See Table 4-1 for COBIT 4.1 control recommendations.

Table 4-1 COBIT 4.1 recommendations

Domain	Process Reference	Process Name and Description	Control Objective Reference	Control Objective Description	Applicability
Deliver and Support	DS7	Effective education of all users of IT systems	DS7.1	Identification of education and training needs	Banks should conduct assessments in order to identify those issues of which the home users of online banking need to be made aware, such as threats, countermeasures, consequences of a breach, incident reporting procedures and expected response times.
			DS7.2	Delivery of training and education	Banks should identify the home users of online banking as a target audience and decide how to deliver the awareness information to the members of this audience. (Delivery methods are outside the scope of this research).
			DS7.3	Evaluation of training received	Banks should conduct surveys on security awareness amongst the home users of online banking after the implementation of an ISA programme. This should serve as an input for improving the subsequent ISA programme.
Plan and Organise	PO7	**Input to DS7:** Users' skills and competencies, including individual training; specific training requirements			This process is aimed at managing the human resources within an organisation and ensuring they are competent users of the organisation's IT systems. In the context of this research, this process is applicable as it recommends that the bank formally identify those aspects that the home users of online banking need to be educated on. Such aspects may include threats, countermeasures and incident reporting procedures.

Domain	Process Reference	Process Name and Description	Control Objective Reference	Control Objective Description	Applicability
Acquire and Implement	AI4	**Input to DS7:** Training materials, knowledge transfer requirements for solution implementation			This process includes control objective AI4.3 which deals with knowledge transfer to end users. Banks should ensure their ISA programmes include current information on threats and countermeasures and that this information is transferred to the home users of online banking.
Deliver and Support	DS1	**Input to DS7:** Service Level Agreements (SLAs)			This process deals with internal service level agreements between IT and business. Banks should commit to a predetermined turnaround time for responses to incidents or concerns reported by the home users of online banking. Home users should be made aware of incident reporting procedures and the expected response times through ISA programmes.
Deliver and Support	DS5	**Input to DS7:** Specific training requirements on security awareness			This process deals with the need to manage security. Part of security management entails an increase in security awareness. Although training does not fall within the scope of this research, banks should identify, and make home users aware of, the threats they face during online banking, what they are able to do to protect themselves and how they should report incidents.

Domain	Process Reference	Process Name and Description	Control Objective Reference	Control Objective Description	Applicability
Deliver and Support	DS8	**Input to DS7:** User satisfaction reports			Banks should conduct a survey amongst home users on their level of satisfaction with the response to reported online banking incidents. The results should be used to improve the incident response procedure. Home users of online banking should be made aware of new incident reporting procedures and incident response times.

4.3.2 ISO/IEC 27001

The ISO 27000 series consists of ISO 27001 and ISO 27002. BS7799 was a standard published in 1995, which then evolved into ISO/IEC 17799:2005 − published in December 2000. This standard was renamed ISO 27002 and published on 16 June 2005. BS 7799-2 was published in 1998 and evolved into ISO 27001, published on 18 October 2005. ISO 27001 is aligned with ISO 27002. ISO 27002 supports ISO 27001 by offering implementation guidance for the control recommendations set out in ISO 27001 (ISO 27000 Directory, 2010). An organisation is said to be certified against ISO 27001. ISO 27001 consists of 11 control sections, 39 control objectives, and 134 controls. ISO 27001 contains the recommendations for establishing an information security management system. These recommendations are mandatory should an organisation wish to be certified against this standard. In view of the fact that an organisation is officially credited with the control objectives and controls as set out in ISO 27001, for the purposes of this research, the focus will be on these control objectives and controls as set out in ISO 27001.

ISO 27001 controls are applicable to most organisations in most environments. Typically, organisations which implement ISO 27001 include the following:

- organisations that view information and the related technology as important business assets
- organisations which want adequate security measures in place to minimise security risks, for example, the protection of trade secrets and client information
- organisations which enable online business services such as online banking

ISO 27001 was developed by business organisations such as Marks & Spencer, Unilever, Lloyds TSB and Nationwide Building Society. Lloyds TSB and Nationwide Building Society are both financial institutions. While it is possible to comply with the standard, proof of compliance through an accredited body provides a way of showing partners, suppliers, staff and customers that the organisation concerned is

taking a stern approach to the management of information security (Adviza Consultants, 2009).

ISO 27001 has been referred to in numerous books and articles, in particular, those addressing information security risks and management. These articles include:

- "State-of-the-art information security management systems with ISO/IEC 27001:2005" (Humphreys, 2006)
- "Information security requirements: interpreting the legislative aspects" (Gerber & von Solms, 2008)
- "Emerging issues in IT governance: implementing the corporate risks IT management model" (Spremic & Popovic, 2008)
- "Information security based on ISO 27001/ISO 17799: a management guide", (Calder, 2009)

The objective of ISO 27001 is to guide the creation of an effective information security management system within an organisation which is aimed at the employees and at protecting both the organisation and its information assets. ISO 27001 also includes those contractors and third party users who require access to an organisation's information technology and information assets. It does not explicitly mention home users. Nevertheless, home users may be regarded as the end users of the internet banking service in the same way that employees may be regarded as the end users of an organisation's systems and applications. Accordingly, controls which pertain to end user security awareness will be included in this research study. Control objectives and the associated controls will be analysed and interpreted in the context of this research under the "Applicability" column. See Table 4-2 for ISO 27001 control recommendations.

Table 4-2 ISO/IEC 27001 Recommendations

Control Section Reference and Name	Control Objective Reference and Name	Control Objective	Control Reference and Name	Control Description	Applicability
A.8 – Human resources security	A.8.2 – During Employment	To ensure employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organisational security policy in the course of their normal work and to reduce the risk of human error.	A.8.2.2 – Information security awareness, education and training	All employees of the organisation and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organisational policies and procedures, as relevant to their job function.	Banks should identify the home users of online banking as a target audience for an ISA programme and, through this ISA programme, these home users should be made aware of the threats they face as online bankers, countermeasures they may implement and an incident reporting procedure they may follow.
A.10 – Communications and operations management	A.10.4 – Protection against malicious and mobile code	To protect the integrity of software and information	A.10.4.1 – Controls against malicious code	Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures should be implemented	Banks should make the home users of online banking aware of ways in which they may protect their information by enabling them to identify hacking attempts, countermeasures they may implement to prevent malicious code from being installed on their computers and incident reporting procedures.

Control Section Reference and Name	Control Objective Reference and Name	Control Objective	Control Reference and Name	Control Description	Applicability
A.10 – Communications and operations management	A.10.8 – Exchange of information	To maintain the security of the information and software exchanged within an organisation and with any external entity.	A10.8.1 – Information exchange policies and procedures	Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities.	Banks should make the home users of online banking aware of ways in which they may protect their information by enabling them to identify hacking attempts such as phishing, social engineering and installation of malicious code and also of the countermeasures they may implement, such as personal firewalls and antivirus software.
A.13 – Information security incident management	A.13.1 – Reporting information security incidents and weaknesses	To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.	A.13.1.1 – Reporting information security events	Information security events should be reported through appropriate management channels as quickly as possible.	Banks should make home users aware of the procedure they should follow when reporting either an information security incident or else a breach of their online banking account.
A.13 – Information security incident management	A.13.2 – Management of information security incidents and improvements	To ensure a consistent and effective approach is applied to the management of information security incidents	A.13.2.1 – Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	Banks should make home users aware of both the procedure to follow should they need to report a breach in their online banking account and also the expected response times.

4.3.3 The Standard of Good Practice for Information Security

The Standard of Good Practice for Information Security is produced by the Information Security Forum (ISF). The standard was first released in 1996. However, the version referred to in this research was released in 2007. The standard is updated every two years and its main objectives include

- meeting the security needs of leading international organisations
- improving information security best practices
- demonstrating thought leadership and addressing the latest security topics
- leveraging off and aligning with international standards such as ISO 27002 and COBIT v4.1.

The standard consists of the following 6 aspects: Security Management (enterprise-wide), Critical Business Applications, Computer Installations, Networks, Systems Development and End User Environment. Each aspect is divided into areas with each area consisting of sections and statements. This research will focus on the aspect of End User Environment. The target audience for the End User Environment aspect includes individuals in the end user environment as well as information security co-ordinators and managers.

The standard may be implemented in any organisation which wants to improve its level of security and reduce its levels of risk by promoting good security practices.

The standard has been referred to in those published articles which mainly address the assessment of information security within organisations. These articles include

- "Information security policy: what do international information security standards say?" (Höne & Eloff, 2002)
- "Assessment of enterprise information security: an architecture theory diagram definition" (Johansson & Johnson, 2005)

- "A prototype for assessing information security awareness" (Kruger & Kearney, 2006)
- "Information security standards focus on the existence of process, not its content" (Siponen, 2006)

Despite the fact that the standard does not explicitly mention home users, for the purpose of this research, the content which addresses user awareness amongst end users will be analysed. The objective of each section of the standard may be seen as a control objective with the statements being seen as controls. Sections and statements will be analysed and interpreted in the context of this research under the "Applicability" column. See Table 4-3 for the control recommendations as set out by the Standard of Good Practice for Information Security.

Table 4-3 The Standard of Good Practice for Information Security recommendations

Section Reference and Name	Section Principle	Section Objective	Statement Reference	Applicability
UE1.2 – Security awareness	Users should be made aware of the key elements of information security and why it is needed, and understand their personal information security responsibilities.	To ensure users apply security controls and prevent important information from being compromised or disclosed to unauthorised individuals.	UE1.2.1	This statement addresses increasing the awareness on the part of employees, contractors and third party users of the organisation's systems and also enabling them to demonstrate compliance with the organisational information security policy. Despite the fact that it does not explicitly mention home users, however, a bank should make home users aware of, and also require them to comply with, certain security recommendations before signing up for online banking. Such recommendations may involve installing antivirus software or ensuring that a strong password is chosen.
			UE1.2.2	Banks should ensure that the security awareness programme reaches all the home users of online banking.
			UE1.2.3	Banks should ensure that the ISA programme succeeds in making home users aware of the information security policy, the importance of both information security and compliance with security recommendations, the consequences of non-compliance as well as measures home users may take to protect themselves.
			UE1.2.4	This statement deals with employees being overheard discussing business information in public places. Banks should make home users aware of the consequences should they divulge confidential information pertinent to their online banking account.
			UE1.2.5	Banks should make home users aware of the threats they face as online bankers, how to identify these threats and the countermeasures they may implement in order to protect themselves.

Section Reference and Name	Section Principle	Section Objective	Statement Reference	Applicability
			UE1.2.6	Banks should ensure home users know how to keep information pertinent to their online banking account confidential. For example, home users should be warned not to compromise their passwords by writing them down.
			UE1.2.7	Banks should ensure home users are aware of, and implement, security controls when conducting online banking. Such controls include the selection of a strong password for their online banking account as well as installing and updating antivirus software.
UE1.3 – User training	Users should be trained in how to run systems correctly and how to develop and apply security controls.	To provide users with the skills required to protect systems and fulfil their information security responsibilities.	UE1.3.1	Banks should offer, and make home users aware of, a tutorial on how home users may set up and secure their online banking accounts.
			UE1.3.2	Banks should make home users aware of the countermeasures they may implement and how to implement these countermeasures.
			UE1.3.3	Not applicable to this research.
UE1.4 – Local security co-ordination	An individual should be appointed to co-ordinate information security activities in the end user environment.	To ensure that security activities are carried out in a timely and accurate manner, and that security issues are resolved effectively.	UE1.4.1	Banks should make home users aware that an individual has been assigned the responsibility of carrying out the ISA programme aimed at the home users of online banking. This will, in turn, help create the impression that that the bank is concerned about the safety of its online bankers.

Section Reference and Name	Section Principle	Section Objective	Statement Reference	Applicability
			UE1.4.2	Not applicable to this research.
			UE1.4.3	Banks should make home users aware that a competent team has been assigned to implementing the ISA programme aimed at the home users of online banking.
			UE1.4.4	Banks should make home users aware that the team responsible for the ISA programme aimed at the home users of online banking meet on a regular basis to discuss improvements and updates to the ISA programme.
UE5.1 – General controls	The use of electronic communications (eg e-mail, instant messaging, Internet access, voice over IP or wireless access) should be supported by setting policy covering the types of communication permitted, and promoting user awareness of the security issues associated with their use.	To ensure that the organisation's reputation is not damaged as a result of the transmission of inappropriate information, that the content of electronic communications is accurate, and that business activity is not disrupted by the introduction of malware.	UE5.1.1	Banks should make home users aware of how to distinguish between legitimate email messages and those email messages which are attempts at social engineering, phishing or the installation of malware.

Section Reference and Name	Section Principle	Section Objective	Statement Reference	Applicability
			UE5.1.2	Not applicable to this research.
			UE5.1.3	Banks should ensure that home users are aware of the security features available to apply to their outgoing email and how to control incoming email.
UE6.1 – Information privacy	Approved methods for handling personally identifiable information should be established and applied.	To prevent information about individuals being used in an inappropriate manner, and to ensure compliance with legislative and regulatory requirements for information privacy.	UE6.1.1	Banks should make home users aware of what action they may take to ensure the information privacy of sensitive information which is pertinent to their online banking account.
			UE6.1.2	Not applicable to this research.
			UE6.1.3	Banks should make home users aware of the sound practices implemented by the banks when handling home users' personal information so as to ensure peace of mind and confidence in the bank itself.
			UE6.1.4	Banks should make home users aware of the relevant legislation they comply to when handling the home users' personal information.

Section Reference and Name	Section Principle	Section Objective	Statement Reference	Applicability
UE6.2 – Information security incident management	Information security incidents should be identified, responded to, recovered from, and followed up using an information security incident management process.	To identify and resolve information security incidents effectively, minimise their business impact and reduce the risk of similar information security incidents occurring.	UE6.2.1	Banks should make home users aware of the procedures they should follow when reporting an information security incident such as a phishing attack or a breach of their online banking account. Home users should be aware of expected response times and the feedback they may expect to receive upon resolution of the incident.
			UE6.2.2	Banks should make home users aware of whom to contact when reporting an information security incident. In addition, banks should log reports and classify them according to the severity.
			UE6.2.3	Not applicable to this research.
			UE6.2.4	Not applicable to this research.
			UE6.2.5	Banks should make home users aware that they will receive feedback once their information security incident has been resolved.
			UE6.2.6	Security incidents should be reviewed and this information used to update any subsequent ISA programmes aimed at the home users of online banking.

4.4 The Best Practice Recommendations List

The most frequently mentioned recommendations are all aimed at making users aware of the threats they face, how they may counteract these threats and also of procedures for reporting incidents. Table 4-4 presents a summary of the recommendations with relevant best practice references mapped to each recommendation. The best practice recommendations include the following:

- Banks should identify what the home users of online banking need to be made aware of through the medium of an ISA programme, for example, threats and countermeasures.
- Banks should identify the home users of online banking as a target audience for user awareness programmes and also ensure that awareness materials reach all home users of online banking.
- Banks should conduct surveys on security awareness amongst the home users of online banking after the implementation of an ISA programme. These findings should serve as an input for improving the next ISA programme.
- Banks should make home users aware of incident reporting procedures and expected response times.
- Banks should conduct a survey amongst home users on their level of satisfaction with the response to reported online banking incidents. These results should be used to improve the incident response procedure. In addition, the home users of online banking should be made aware of new incident reporting procedures and incident response times.
- Banks should make the home users of online banking aware of ways in which they may protect their information.
- Banks should make home users aware of, and require them to comply with, certain security requirements stipulated in an information security policy before signing up for online banking.
- Banks should demonstrate to the home users of online banking that they take a stern approach to information security management and awareness.

Table 4-4 Best Practice Recommendations Summary

	BEST PRACTICE / INTERNATIONAL STANDARD REFERENCE		
RECOMMENDATION	COBIT 4.1 (Control Objective Reference)	ISO 27001 (Control Reference)	The Standard of Good Practice for Information Security (Statement Reference)
Banks should identify what home users of online banking need to be made aware of through the ISA programme, such as threats and countermeasures	(DS7.1) (PO7 – Input to DS7) (DS5 – Input to DS7)	(A.8.2.2)	(UE1.2.3) (UE1.2.5) (UE1.2.7) (UE1.3.2) (UE5.1.1) (UE5.1.3)
Banks should identify the home users of online banking as a target audience for user awareness programmes and also ensure that awareness materials reach all home users of online banking	(DS7.2) (AI4 – Input to DS7)	(A.8.2.2)	(UE1.2.2)
Banks should conduct surveys on security awareness amongst the home users of online banking after the implementation of an ISA programme. These findings should serve as an input for improving the next ISA programme	(DS7.3)		
Banks should make home users aware of incident reporting procedures and expected response times	(DS1 – Input to DS7)	(A.13.1.1) (A.13.2.1)	(UE6.2.1) (UE6.2.2) (UE6.2.5)

	BEST PRACTICE / INTERNATIONAL STANDARD REFERENCE		
RECOMMENDATION	COBIT 4.1 (Control Objective Reference)	ISO 27001 (Control Reference)	The Standard of Good Practice for Information Security (Statement Reference)
Banks should conduct a survey amongst home users on their level of satisfaction with the response to reported online banking incidents. These results should be used to improve the incident response procedure. In addition, the home users of online banking should be made aware of new incident reporting procedures and incident response times	(DS8 – Input to DS7)		(UE6.2.6)
Banks should make the home users of online banking aware of ways in which they may protect their information		(A.10.4.1) (A.10.8.1)	(UE1.2.4) (UE1.2.6) (UE1.3.1) (UE6.1.1)
Banks should make home users aware of, and require them to comply with, certain security requirements stipulated in an information security policy before signing up for online banking			(UE1.2.1) (UE1.2.3)
Banks should demonstrate to the home users of online banking that they take a stern approach to information security management and awareness			(UE1.4.1) (UE1.4.3) (UE1.4.4) (UE6.1.3) (UE6.1.4)

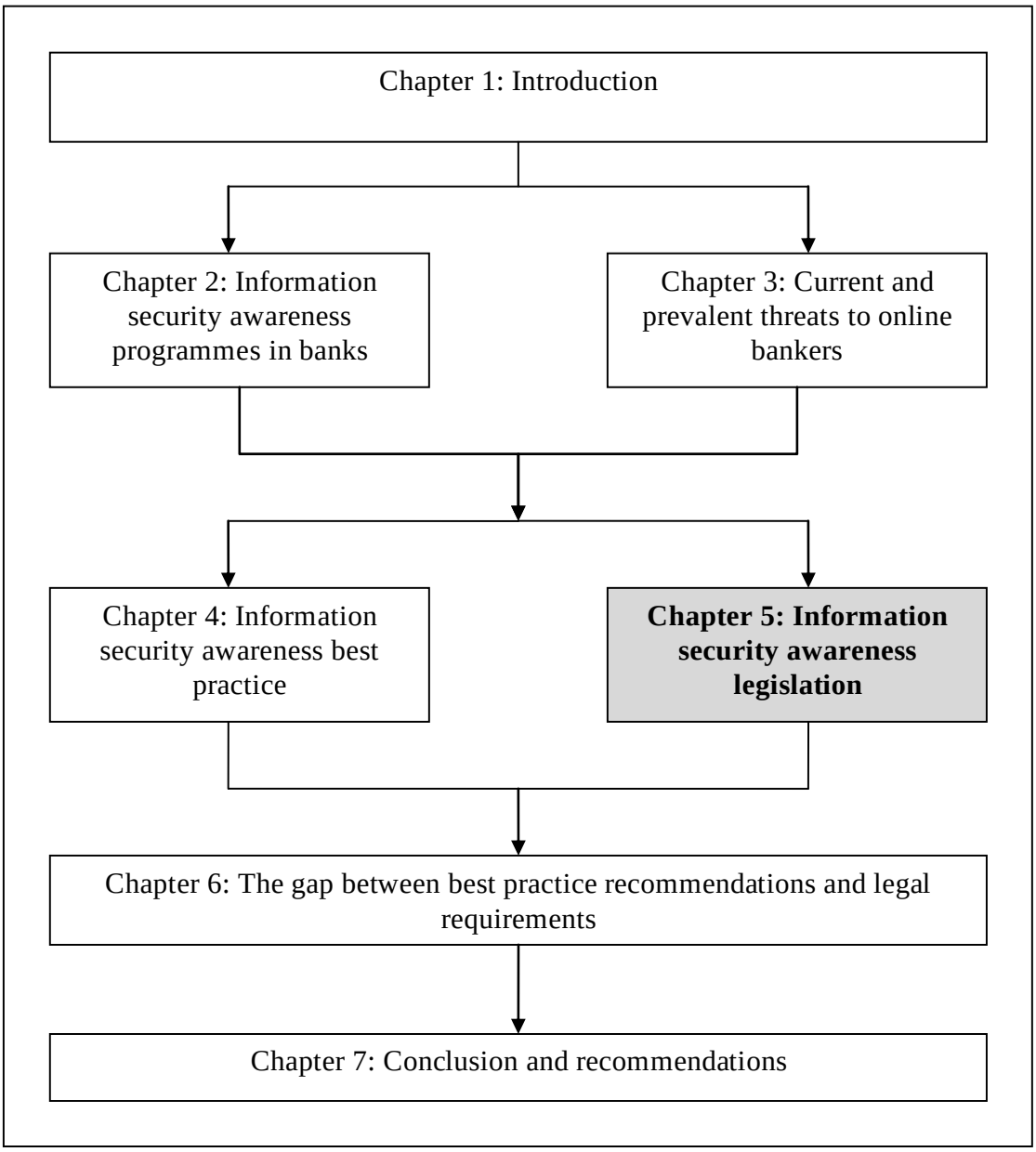
4.5 Summary

In this chapter, a number of selected, internationally recognised information security best practices were identified and an investigation undertaken to ascertain what recommendations these international standards offer to organisations regarding user awareness. Each requirement was analysed to gain an understanding of what an ISA programme aimed at the home users of online banking would need to include to satisfy best practice recommendations. The final result comprised a list of information security best practices which should be implemented when devising an ISA programme aimed at the home users of online banking. Despite the fact that the list of selected best practices is not exhaustive it is, nevertheless, sufficient as it satisfies the criteria for appropriate best practices for this research.

In the next chapter, Chapter 5, a similar investigation is undertaken, but with the focus on the requirements which selected laws and regulations, pertinent to South African banks, impose on banks in respect of home user awareness. These requirements are extracted and analysed to gain an understanding of what the content of an ISA programme aimed at home users of online banking would need to include to satisfy these legal requirements. The culmination of this chapter is a final list of legal requirements which a bank must fulfil through an ISA programme aimed at the home users of online banking. In Chapter 6, a comparison is made between the best practice recommendations identified and the legal requirements identified to uncover any significant gaps between the two.

Chapter 5:

Information Security Awareness Legislation


Chapter 1: Introduction
Chapter 2: Information security awareness programmes in banks
Chapter 3: Current and prevalent threats to online bankers
Chapter 4: Information security awareness best practice
Chapter 5: Information security awareness legislation
Chapter 6: The gap between best practice recommendations and legal requirements
Chapter 7: Conclusion and recommendations

5.1 Introduction

The Internet provides the infrastructure for various online products and services aimed at home users with access to the Internet. These products and services include online banking which is a form of banking affording home users the opportunity to complete banking transactions online, for example, transferring money and paying accounts. Online banking is convenient, but has numerous information security threats associated with its use − see Chapter 3. The existence of these information security threats and their consequences has motivated the need for regulation within the banking industry. Accordingly, information security has, increasingly, become the subject of national and global legislation (Gerber & von Solms, 2008). In Chapter 4, selected information security best practices and international standards were analysed for information security awareness (ISA) recommendations. In this chapter, the legal requirements for information security awareness in selected legal documents are analysed. The aim of this analysis is to identify the obligations which South African banks have towards the home users of online banking when implementing an ISA programme.

There is a close link between information security best practice and the legal requirements for information security, thus making it difficult to separate the two (British Standards Institution, 2005; King Committee on Governance, 2009). For example, in control section A.15, international best practice ISO/IEC27001 deals with compliance with legal requirements, including laws, regulations, statutes and contractual obligations. In this vein, compliance with legal requirements may be achieved by implementing best practice recommendations, for example, the implementation of COBIT to comply with Sarbanes-Oxley. Compliance ensures that, should a legal breach occur, the organisation concerned will be able to demonstrate due care and due diligence, and, thus, avoid both financial and legal consequences (von Solms & von Solms, 2004; Williams, 2008).

5.2 Documents to be Analysed

The objective of the analysis is to draw up a list of the legal requirements which it is incumbent on South African banks when implementing an ISA programme aimed at

the home users of online banking. The documents consulted in this chapter include selected laws, regulations, statutes and contractual obligations which have information security implications for South African banks. A law refers to a rule or system of rules imposed by a government to regulate society and it normally carries consequences for noncompliance. Laws include regulations − imposed and maintained by a relevant authority − and statutes, which are written laws such as an Act and which are formally passed by a legal body. Laws may also enforce contractual obligations, which are acts a party is obliged to perform, as stated in a contract (*Cambridge Dictionaries Online*, 2011[a]; *Oxford English Dictionary*, 2011[a]).

This chapter offers both an introduction and a description of its objective for each selected law, regulation, statute and contractual obligation. Information security requirements are extracted and analysed for the obligations which South African banks have towards the home users of online banking when implementing an ISA programme.

Mra Khwar Nyo is an attorney and Certified Information Privacy Professional (International Association of Privacy Professionals) working in the Security and Privacy Services team at Deloitte & Touche, South Africa. Mra was consulted for her opinion as to which legislation should be included in this research. She recommended international banking legislation and South African legislation and also suggested other relevant documents. A visit to the South African government's website for documents available to the public was carried out to research other pertinent documents and to identify relevant amendments to the final list of documents. The legislation identified includes the following:

- Basel II
- Sarbanes-Oxley Act of 2002
- Gramm-Leach-Bliley Act of 1999
- Electronic Communications and Transactions Act, 2002
- Protection of Personal Information Bill
- Promotion of Access to Information Act, 2000

- The Code of Banking Practice
- Consumer Protection Act, 2008
- Constitution of the Republic of South Africa
- Code of Governance Principles for South Africa (King III), 25 February, 2009
- Electronic Communications Act, 2005

The selected documents listed will now be analysed in detail for the ISA requirements which they impose on banks.

5.3 Compiling the Legal Requirements List

In this section, each legal document is introduced, described and analysed for requirements. These requirements are illustrated in a table which presents the legal requirements which the legal documents impose on banks when the banks implement an ISA programme aimed at the home users of online banking. Depending on the activities of the bank, the applicability of the legal requirements may vary. For example, Basel II is applicable to banks which carry out international activities. For this reason, the list of legal requirements will be sectioned into the relevant laws, regulations, statutes and contractual obligations.

This sectioned list of legal requirements was merged and duplicates removed. The resultant list is then compared to the final list of best practice recommendations as identified in Chapter 4. Any overlaps and gaps are identified and presented in Chapter 6. For this merged table, the assumption is that the bank would need to comply with all the legal requirements as identified in this research.

5.3.1 BASEL II

Basel II is a framework presented by the Basel Committee on Banking Supervision, and relevant to all banks which conduct international business activities (Basel Committee on Banking Supervision, 2004). Basel II offers recommendations for national banking regulators worldwide when regulating the calculation of capital requirements for banks. Basel II encourages banks to adopt a risk management approach to business. The fact that Basel II focuses on operational risk and classifies information security as part of the operational risk management system is important in the context of this research. The Basel Committee has identified operational risks which have the potential to cause significant losses. These operational risks include fiduciary breaches, theft by employees, misuse of confidential customer information and hacking (Basel Committee on Banking Supervision, 2004). For the purposes of this research, hacking constitutes the relevant operational risk. Operational risk falls under Pillar I: Minimum Capital Requirements of Basel II. For guidance on operational risk management, the Basel Committee refers to the document "Sound practices for the management and supervision of operational risk", February 2003. In this document, the committee has categorised operational risk events. "External Fraud", which includes damages from hacking, is the category which is relevant to this research.

Pillar III: Market Discipline imposes disclosure requirements on banks within each risk area, including operational risk. The Pillar I guidance document "Sound Practices for the management and supervision of operational risk" and paragraph 824 of Pillar III will be analysed for the requirements they impose on banks when banks implement an ISA programme aimed at the home users of online banking. These requirements are presented in Table 5-1.

Table 5-1 BASEL II Requirements

Reference	Requirement
"Sound practices for the management and supervision of operational risk", February 2003 Principle 1, paragraph 12	Banks should make home users aware of their approach to identifying and mitigating risks facing them when participating in online banking.
"Sound practices for the management and supervision of operational risk", February 2003 Principle 1, paragraph 15	Banks should review risks facing home users of online banking and make appropriate changes to its risk mitigating processes, including the content of the ISA programme.
"Sound practices for the management and supervision of operational risk", February 2003 Principle 2, paragraphs 16 and 17	Banks should assure home users of online banking that the effectiveness of controls implemented to mitigate risks facing them are reviewed by an independent auditor.
"Sound practices for the management and supervision of operational risk", February 2003 Principle 4, paragraphs 23, 24 and 25	Banks should identify all risks facing home users of online banking and make home users aware of how they can mitigate these risks.
"Sound practices for the management and supervision of operational risk", February 2003 Principle 5, paragraphs 26, 27, 28, 29 and 30	Banks should implement controls to mitigate new threats to home users of online banking and, where appropriate, update the ISA programme to include these new threats.

Reference	Requirement
"Sound practices for the management and supervision of operational risk", February 2003 Principle 6, paragraphs 32, 34, 37 and 38	• The board of directors and senior management at banks should demonstrate to the public a stern stance on information security • Banks should make home users of online banking aware of information security technology they can implement to mitigate risks, and, where possible, make this technology available to home users. An example of such a technology would be software which checks the home user's antivirus software and notifies the home user if it offers sufficient protection when online banking
"Sound practices for the management and supervision of operational risk", February 2003 Principle 1, paragraphs 50 and 51	The bank should make timely and frequent public disclosures of information which will assist the public to determine how effective a bank is at risk identification, assessment, monitoring and control.
BASEL II, June 2004, paragraph 824	**General qualitative disclosure requirement** Banks must describe their risk management objectives and policies.

Basel II requires banks to adopt a risk management approach to business. Information security is addressed through the implementation of an effective operational risk management framework which is supported by senior management. Despite the fact that Basel II does not explicitly include a requirement for an ISA programme aimed at the home users of online banking it does, however, imply this in its requirement in respect of the identification and management of risks associated with external fraud and banking products. Banks may consult security best practices/international standards for guidance on risk mitigation, which reveal the need for an effective ISA programme.

5.3.2 Sarbanes-Oxley Act of 2002

The Sarbanes-Oxley Act of 2002, referred to in this section as "the Act", was created in response to a number of corporate fraud cases. The main objective of this Act is to hold the board of directors responsible for the release of financial reports which accurately present and validate the performance of an organisation (The Institute of Internal Auditors, 2008). The Act is pertinent to all American and international companies with registered equity or debt securities with the Securities and Exchange Commission. Included in its requirements, the Act requires compliance with a set of internal controls to ensure accurate financial reporting (SOX-online, 2009). Section 404 of the Act is concerned with management's assessment of the internal controls over financial reporting. Firstly, management is made formally accountable for implementing and maintaining an effective internal control structure. Secondly, Section 404 requires that this internal control structure be independently audited at the end of each fiscal year. Several business processes rely on information technology (Ugochuku, 2006) which necessitates that the internal control structure incorporates an information security aspect.

Computer controls in scope for the assessment of the internal control structure include general computer controls and application controls. General controls are those controls which ensure that the information output of an information technology (IT) system is accurate for financial reporting (SANS, 2011). General controls in scope for an audit of the internal control structure are those which support application controls which have a bearing on accurate financial reporting. General computer controls which are designed for the effectiveness and efficiency of business operations are excluded from the audit (The Institute of Internal Auditors, 2008). Application controls refer to those automated controls within the software applications which are used either to create or make changes to data for the purposes of financial reporting (SANS, 2011).

The Act does not explicitly address the ISA requirements imposed on banks. However, there are certain guidance documents which do mention awareness, for example, efforts to make management and employees aware of the security policy and

their responsibilities when enforcing controls within the organisation (SANS, 2011; The Institute of Internal Auditors, 2008). The Act would require the implementation of an ISA programme aimed at the home users of online banking if the systems which facilitate online banking were justified as within scope of the audit of the internal control structure for accurate financial reporting, the Section 404 assessment and if the scope of key controls included the implementation of such a programme. A key control refers to a control that, should it fail, will result in a material error in the financial reports. Key controls preventing fraud should be considered in scope only if such fraud would result in a material misstatement of the financials. A misstatement is considered material if it would affect the decision of a reasonable person who was considering investing in the bank concerned (The Institute of Internal Auditors, 2008).

For the purposes of this research, it is assumed both that the systems supporting online banking are considered in scope for the Section 404 assessment and that the key controls identified include the implementation of an awareness programme aimed at the home users of online banking. If a bank were to meet the control requirements, the bank could implement the relevant COBIT controls (The Institute of Internal Auditors, 2008; Ugochuku, 2006). Drawing from Chapter 4, the requirements imposed on banks when satisfying a Section 404 assessment on its online banking system, with the implementation of an ISA programme aimed at the home users of online banking identified as a key control, are presented in Table 5-2.

Table 5-2 Sarbanes-Oxley Act of 2002 Requirements

Reference	Requirement
COBIT 4.1 Control Objective References: DS7.1 PO7 – Input to DS7 DS5 – Input to DS7	Banks should identify what home users of online banking need to be made aware of through the ISA programme, such as threats and countermeasure
COBIT 4.1 Control Objective References: DS7.2 AI4 – Input to DS7	Banks should identify home users of online banking as a target audience for user awareness programmes and ensure awareness materials reach all home users of online banking
COBIT 4.1 Control Objective References: DS7.3	Banks should conduct surveys on security awareness amongst home users of online banking after the implementation of an ISA programme. This should serve as an input for improving the next ISA programme
COBIT 4.1 Control Objective References: DS1 – Input to DS7	Banks should make home users aware of incident reporting procedures and expected response times
COBIT 4.1 Control Objective References: DS8 – Input to DS7	Banks should conduct a survey amongst home users on how satisfied they are with the response to reported online banking incidents. The results should be used to improve the incident response procedure. Home users of online banking should be made aware of new incident reporting procedures and incident response times

5.3.3 Gramm-Leach-Bliley Act of 1999

The Glass-Steagall Act of 1933 prohibited financial institutions from functioning as commercial banks, investment banks and insurance companies in one. The Gramm-Leach-Bliley Act of 1999, referred to in this section as "the GLB Act" − also known as the Financial Services Modernization Act of 1999 − was intended to repeal the Glass-Steagall Act. By allowing the combination of commercial banking, investment banking and insurance services under one service provider the enactment of the GLB Act meant that the American financial industry was able to become more competitive within the global market (Neale & Peterson, 2005). Like Basel II and the Sarbanes-Oxley Act of 2002, the Gramm-Leach-Bliley Act of 1999 is relevant to those banks which conduct international banking activities.

The privacy of online transactions and personal information are not only matters of major concern but they also constitute barriers to the acceptance of online banking on the part of home users (Gikandi & Bloor, 2009; Laukkanen, Sinkkonen & Laukkanen, 2009). Compliance requirements for privacy and security of client information are addressed by the GLB Act through the Financial Privacy Rule, the Safeguards Rule and Pretexting Protection. The Financial Privacy Rule and the Safeguards Rule are addressed by Subtitle A: Disclosure of Nonpublic Personal Information while Pretexting Protection is addressed by Subtitle B: Fraudulent Access to Financial Information. Pretexting is often referred to as social engineering and may result from the phishing technique. As such, pretexting is an attempt to gain confidential information in an unauthorised manner. It may be done telephonically, via email or a spoofed website. Social engineering and phishing techniques were identified in Chapter 3 as threats facing the home users of online banking.

The GLB Act makes an important distinction between customers and consumers. According to the GLB Act, a consumer is a person who obtains a product or service from a financial institution for personal, family or household purposes while a customer is a consumer who has a continuing relationship with a financial institution. Under the GLB Act, the bank has different obligations to customers and to consumers. For the purposes of this research, the home user of online banking will be classed as a

customer. In this section, Subtitle A, sections 6801-6809 and Subtitle B, and sections 6821-6827 in the GLB Act will be analysed for the ISA obligations which banks have towards their online banking customers.

Subtitle A, sections 6801–6809, deals with both the Financial Privacy Rule and the Safeguards Rule. The Financial Privacy Rule addresses the collection and disclosure of customers' personal financial information while the Safeguards Rule addresses the need for a bank to have in place a documented security plan which communicates how the bank concerned intends to protect its customers' information. Subtitle B, sections 6821-6827, deals with Pretexting Protection. The GLB Act requires banks to plan and implement controls against pretexting. The awareness requirements imposed on banks by the GLB Act, when complying with Subtitle A and Subtitle B, are presented in Table 5-3.

Table 5-3 The Gramm-Leach-Bliley Act of 1999 Requirements

Reference	Requirement
Subtitle A, Section 6801	Banks should make online banking customers aware of the bank's stance on privacy of customers' non-public, personal information.
	Banks should implement an information security plan and standards to protect the security and privacy of customer information, to protect the integrity of customer information from threats and to protect customer information from unauthorised access. This security plan should include an awareness programme aimed at customers of online banking, informing them of the threats relevant to them and countermeasures they may implement to protect themselves.
Subtitle A, Section 6802	Banks should make customers aware of the circumstances under which their non-public, personal information will be shared, how they will be notified and their opt-out options.
Subtitle A, Section 6803	Banks should make customers aware of their privacy policy, dealing with disclosure and protection of customers' non-public personal information. This should be done upon initiation of the customer relationship and annually thereafter until the relationship is terminated.
	Banks should make customers aware of: • The types of organisations their non-public personal information will be shared with • The bank's policy on disclosing current customers' non-public personal information with past customers • The types of customers' non-public personal information collected by the bank • The banks' policy on how it protects the security and confidentiality of customers' non-public personal information
Subtitle B, Section 6821	Banks should make online banking customers aware of the methods used in pretexting, how to identify pretexting and how to respond. For example, make online banking customers aware of the procedure to be followed when reporting a security incident such as a social engineering or phishing attempt.

5.3.4 Electronic Communications and Transactions Act, 2002

On 2 August, 2002, The Electronic Communications and Transactions Act, Act No. 25 of 2002 (referred to in this section as "the Act"), was published after having been agreed to by the President of the Republic of South Africa on 30 July, 2002. The Act became law on 30 August, 2002. The purpose of this act is to regulate electronic transactions, to address the abuse of information systems, and to provide legal guidance where no guidance had existed before. The objects of the act which are relevant to this research include:

- promoting an appreciation and acceptance of the increasing number of electronic transactions in South Africa
- promoting the regulation of and confidence in electronic communications and transactions
- ensuring that all aspects of electronic transactions in South Africa comply with international standards
- developing and maintaining a safe and secure environment within which home and business users, as well as government, may use electronic transactions

The Act comprises fourteen chapters. For the purposes of this research, Chapter VII of the Act − Consumer Protection, and Chapter VIII − Protection of Personal Information, will be analysed. Awareness requirements imposed on banks by the Act are presented in Table 5-4.

Table 5-4 Electronic Communications and Transactions Act, 2002 requirements

Reference	Requirement
Chapter VIII, section 51	Banks should make the home users of online banking aware that their personal information will be collected, stored, processed and released only for lawful purposes and that they will be notified before any such activities take place

5.3.5 Protection of Personal Information Bill, 2009

The Protection of Personal Information Bill, referred to in this section as "the Bill", was published on 25 August, 2009. This Bill is aligned with section 14 of the Constitution of South Africa, stating a person's right to privacy. Banks have a social and legal responsibility to protect the personal information of consumers. Identity theft may result from a criminal's possession of non-public, personal information. As discussed in Chapter 3, the major threats facing the home users of online banking were all associated with identity theft. The Bill requires that organisations which collect and process personal information to do so in a lawful and secure manner. The Bill consists of the following eight information protection principles which will be analysed for the ISA obligations which banks have in respect of their home users of online banking:

- accountability
- processing limitation
- purpose specification
- further processing limitation
- information quality
- openness
- security safeguards
- data subject participation

Awareness requirements imposed on banks by the Bill are presented in Table 5-5.

Table 5-5 Protection of Personal Information Bill, 2009 requirements

Reference	Requirement
Principle 1: Accountability	Not applicable to this research
Principle 2: Processing limitation	Banks should make the home users of online banking aware that only necessary personal information will be collected and processed in a lawful manner, with the consent of the home user
Principle 3: Purpose specification	Banks should make the home users of online banking aware that their personal information will only be collected and processed for legitimate purposes and retained only for as long as required by these purposes. The purposes for collection and processing should be explained to the home user before such collection or processing takes place
Principle 4: Further processing limitation	Banks should make the home users of online banking aware that they will be notified and their consent sought should the bank need to process their personal information for purposes not already specified
Principle 5: Information quality	Banks should make the home users of online banking aware that their personal information will be kept accurate and up-to-date
Principle 6: Openness	Banks should make the home users of online banking aware that they will always be notified of the types of personal information collected about them and the purpose for which it is being collected and processed
Principle 7: Security safeguards	• Banks should make the home users of online banking aware of the efforts made by the banks to keep personal information safe from loss, unauthorised access and either unlawful processing or disclosure • Banks should also make home users aware of the countermeasures they may implement in order to protect their personal information • Banks should make the home users of online banking aware that they will be notified if it has been established that their personal information has been compromised
Principle 8: Data subject participation	Banks should make home users aware that they are entitled to confirm what personal information is held for the purpose of online banking as well as update or delete, or request to be updated or deleted, personal information held by the bank for the purpose of online banking

5.3.6 Promotion of Access to Information Act, 2000

On 3 February 2000, the Promotion of Access to Information Act, Act No. 2 of 2000, referred to in this section as "the Act", was published after having been agreed to by the President of the Republic of South Africa on 2 February, 2000. The purpose of this act is to regulate access to information held by either a public or a private body. The Act addresses the access to information held by a public body separately to the access to information held by a private body. A bank is not a department of state and is considered to be a private body. The requirements as stipulated in Part 3: Access to Records of Private Bodies of the Act are analysed for the ISA obligations which a bank has towards its home users of online banking. The Act should be read together with the laws repealed and amended in the Schedule of the Protection of Personal Information Bill, 2009. The awareness requirements imposed on banks by the Act are presented in Table 5-6.

Table 5-6 Promotion of Access to Information Act, 2000 requirements

Reference	Requirement
Part 3, Section 63	Banks should make the home users of online banking aware that banks will not unreasonably disclose the home user's personal or financial information in answer to any requestor other than that of the home user
Part 3, Section 71	Banks should make the home users of online banking aware that they will be informed should a requestor, other than the home user, attempt to access either their personal information or their financial information. Banks should also inform home users of their rights to refuse access to their personal information by a requestor

5.3.7 The Code of Banking Practice

The Code of Banking Practice, referred to in this section as "the Code", was released by the Banking Council South Africa and has been in force since 1 October 2004. The Code pertains to dealings between banks and their clients as well as providing safeguards for the clients of banks. The Code is not legally binding, however, should a bank refuse to comply with the Code, the Ombudsman for Banking Services may publish this fact. Such a disclosure may affect consumers' trust in the banking service. In this section 5.3.7, a home user of online banking will be referred to as a personal client. The Code defines a personal client as a natural person who maintains an account or makes use of other services provided by a bank.

Section 3 of the Code outlines the fundamental principles of the bank-client relationship. These principles include the provision of both reliable banking and payment systems to the personal client, with due care being exercised to ensure that these systems remain secure. Section 4: Disclosure of the Code, states that banks will recommend safety measures and tips as pertaining to their services, where relevant. In addition, the Code explicitly addresses internet and telephone banking in section 5.14 (Section 5: Conduct). The Code may hold the personal client liable for losses should he/she either not take reasonable care or fail to comply with the precautions set out in section 5.14. Banks have the option of either making their personal clients who use the online banking service aware of these precautions through the medium of an ISA programme or else making them aware of the existence of the Code through such a programme. The precautions recommended in section 5.14 by the Banking Council South Africa to personal clients using the online banking service are presented in Table 5-7**.**

Table 5-7 Code of Banking Practice requirements

Reference	Requirement
Section 5: Conduct	Banks should inform personal clients using online banking that they review their bank statements and reconcile their accounts on a regular basis
Section 5: Conduct	Banks should recommend to personal clients using online banking never to reveal their online banking password or any unique, personally identifiable information, even to bank staff
Section 5: Conduct	Banks should recommend to personal clients using online banking that they always check the online banking site's security certificate before carrying out their banking
Section 5: Conduct	Banks should recommend to personal clients using online banking that they change a temporary password to a strong password known to the personal client only as soon as possible
Section 5: Conduct	Banks should recommend to personal clients using online banking that they change their password immediately when they suspect its confidentiality has been compromised
Section 5: Conduct	Banks should make personal clients using online banking aware that the security of their personal computers is the responsibility of the personal client
Section 5: Conduct	Banks should recommend to personal clients using online banking that they read and understand the terms and conditions associated with the online banking service before signing up for the service
Section 5: Conduct	Banks should recommend to personal clients using online banking that they take care to enter login and transaction information accurately
Section 5: Conduct	Banks should recommend to personal clients using online banking that they take care to enter accurate transaction information as it is not possible to reverse transactions without the recipient's consent
Section 5: Conduct	Banks should recommend to personal clients using online banking that they disable "remember my password" browser functionality
Section 5: Conduct	Banks should recommend to personal clients using online banking that they install effective antivirus and security software on their personal computers and that they keep this software up to date

5.3.8 Consumer Protection Act, 2008

On 29 April, 2009, the Consumer Protection Act, Act No. 68 of 2008, referred to in this section as "the Act", was published and assented to by the President of the Republic of South Africa. The purpose of the Act is to promote fair business practice in the supply of goods or services to consumers. The law was enacted, inter alia, to protect consumers from risks to their safety and security when receiving goods from suppliers or when benefiting from services. The suppliers of goods and service providers, such as banks, are required to have demonstrated compliance with the Act by 1 April, 2011. The Act refers to the person receiving the goods or benefiting from the service as the consumer. In this section 5.3.8 the home users of online banking will be referred to as consumers. The objectives of the Act are described in Part B of Chapter 1 of the Act. These objectives include the enhancement of consumer awareness and the encouragement of responsible and informed consumer choice and behaviour. By making the home users of online banking aware of the risks they face, as well as how they may mitigate these risks, the banks are playing an important role in protecting their consumers. The awareness requirements imposed on banks in terms of the Act are presented in Table 5-8.

Table 5-8 Consumer Protection Act, 2008 requirements

Reference	Requirement
Chapter 2, Part H, Section 58	Banks should make consumers aware, in simple, unambiguous language, of any risk associated with the online banking service that a generally alert consumer would not expect
Chapter 2, Part H, Section 60	Banks should make consumers aware of incident reporting facilities and procedures

5.3.9 Constitution of the Republic of South Africa

The Constitution of the Republic of South Africa, Act No. 108 of 1996, referred to in this section as "the Constitution", was promulgated on 18 December, 1996 with the intention that it would come into effect on 4 February 1997. The Constitution is the highest law in South Africa with any laws which are in conflict with the Constitution being deemed invalid. Chapter 2 of the Constitution presents the Bill of Rights. Section 14 of the Bill of Rights is relevant to this research as this section states a person's right to privacy. The privacy of an individual's non-public, personal information is addressed in the Protection of Personal Information Bill, 2009, which is aligned with section 14 of the Constitution. The Protection of Personal Information Bill was analysed for the awareness requirements it imposes on banks in section 3.3.5 of this research study. The requirements imposed on banks by the Constitution are presented in Table 5-9**.**

Table 5-9 Constitution of the Republic of South Africa requirements

Reference	Requirement
Section 14	Banks should make the home users of online banking aware both of the existence of threats to the privacy of their non-public, personal information and also of the countermeasures they should implement in order to protect the privacy of their non-public, personal information

5.3.10 Code of Governance Principles for South Africa (King III), 25 February, 2009

The Code of Governance Principles for South Africa, referred to in this section as "King III", comprises a set of corporate governance principles. King III was preceded by King I and King II. Trends and changes in international corporate governance were taken into account when King III was compiled. King III applies to all organisations and an organisation's compliance with this code will result in the practise of good governance. However, should a practice recommended by the code not be implemented by an organisation, this will be deemed acceptable if the board of the organisation is able to explain that the practice which is being implemented instead is a better fit for the organisation and results in compliance. Unlike King I and King II, King III addresses IT governance in detail. King III recognises the significance of the impact which IT risks may have on an organisation and it recommends the implementation of international standards, such as the standards addressed in Chapter 4 of this research, to manage and mitigate IT risks effectively. Chapter 4 of King III deals with risk management. Principle 4.16 covers IT security. This principle is analysed for the awareness requirements imposed on banks when implementing an ISA programme aimed at the home users of online banking. These requirements are presented in Table 5-10.

Table 5-10 Code of Governance Principles for South Africa (King III), 2009 requirements

Reference	Requirement
Principle 4.16	Banks should make the home users of online banking aware that the banks adopt an uncompromising position regarding the security of online banking transactions
Principle 4.16	Banks should make the home users of online banking aware of the threats they face when conducting online banking and also recommend countermeasures which home users should implement to mitigate the associated risks

5.3.11 Electronic Communications Act, 2005

On 18 April 2006, the Electronic Communications Act, Act No. 36 of 2005, referred to in this section as "the Act", was published and assented to by the President of the Republic of South Africa. The purpose of the Act is to provide a legal framework governing the convergence of broadcasting, broadcasting signal distribution and telecommunications sectors. The Act includes social obligations. Section 3(1) of the Act calls for the development of policies that are aligned with and support the objectives of the Act.

Accordingly, on 19 February 2010, a government notice was released by the Department of Communications making public the intention to create the South African National Cybersecurity Policy and to present the Draft Cybersecurity Policy of South Africa. This policy takes into account other legislation in South Africa which impacts on cybersecurity. The objectives of this policy include the encouragement of a joint effort between government and the private sector to create and promote a culture of cybersecurity. The policy anticipates that one of the benefits derived from a secure cyberspace would include a safe and secure cyberspace that the individual would be able both to trust and to use with confidence. Although the policy does not offer guidance on the content of an ISA programme, it does require that such a programme be implemented. The obligations imposed on banks by the policy, in accordance with the Act, when addressing information security awareness amongst the home users of online banking are presented in Table 5-11**.**

Table 5-11 Electronic Communications Act, 2005 requirements

Reference	Requirements
Chapter 6	Banks should promote a culture of cybersecurity by developing and implementing ISA programmes aimed at the home users of online banking

5.4 The Legislation Requirements List

A list of requirements imposed on banks by the selected laws, regulations, statutes and contractual obligations which were investigated in this research are presented in Table 5-12 with the requirements pertaining to these laws, regulations, statutes and contractual obligations being sectioned under the relevant legislation. The final list of legal requirements includes the following 18 requirements:

1. Banks should identify home users of online banking as a target audience for user awareness programmes and ensure awareness materials reach all home users of online banking.
2. Banks should make consumers aware, in plain language, of any risk associated with the online banking service that an ordinarily alert consumer would not expect.
3. Banks should promote a culture of cybersecurity by developing and implementing an ISA programme aimed at home users of online banking.
4. Banks should make home users of online banking aware that they take a stern stance on the security of online banking transactions and privacy of personal information.
5. The bank should make timely and frequent public disclosures of information which will assist the public to determine how effective a bank is at risk identification, assessment, monitoring and control. This should include the use of an independent auditor.
6. Banks should make home users of online banking aware of the threats they face when banking online, including threats to the privacy of their personal information, and recommend countermeasures they should implement to mitigate the associated risks.
7. Banks should make antivirus software available to home users of online banking.
8. Banks should make home users aware of incident reporting procedures and expected response times.

9. Banks should review the content of ISA programmes to include new threats, changes in incident reporting procedures and response times and make home users aware of these new threats.
10. Banks should make home users of online banking aware of their privacy policy, dealing with disclosure and protection of customers' non-public personal information. This should be done upon initiation of the customer relationship and annually thereafter until the relationship is terminated.
11. Banks should make home users of online banking aware that their personal information will only be collected and processed for legitimate purposes and retained only for as long as required by these purposes. The purposes for collection and processing should be explained to the home user before collection or processing takes place.
12. Banks should make home users of online banking aware that they will be notified if it can be established that their personal information has been compromised.
13. Banks should make home users aware that they are entitled to confirm what personal information is held for the purpose of online banking as well as update or delete, or request to be updated or deleted, personal information held by the bank for the purpose of online banking.
14. Banks should make home users of online banking aware that they will be informed should a requestor other than the home user attempt to access their personal information or financial information. The bank should also inform the home user of their rights to refuse access to their personal information by the requestor.
15. Banks should recommend to personal clients using online banking that they review their bank statements and reconcile their accounts on a regular basis.
16. Banks should make personal clients using online banking aware that security of their personal computer is the responsibility of the personal client.
17. Banks should recommend to personal clients using online banking that they read and understand the terms and conditions associated with the online banking service before signing up for the service.

18. Banks should recommend to personal clients using online banking that they be careful to enter accurate transaction information as transactions cannot be reversed without the recipient's consent

Table 5-12 Legal requirements

Legislation	Requirement
BASEL II	Banks should make home users aware of their approach to identifying and mitigating risks facing them when participating in online banking.
	Banks should review risks facing home users of online banking and make appropriate changes to its risk mitigating processes, including the content of the ISA programme.
	Banks should assure home users of online banking that the effectiveness of controls implemented to mitigate risks facing them are reviewed by an independent auditor.
	Banks should identify all risks facing home users of online banking and make home users aware of how they can mitigate these risks.
	Banks should implement controls to mitigate new threats to home users of online banking and, where appropriate, update the ISA programme to include these new threats.
	• The board of directors and senior management at banks should demonstrate to the public a stern stance on information security • Banks should make home users of online banking aware of information security technology they can implement to mitigate risks, and, where possible, make this technology available to home users. An example of such a technology would be software which checks the home user's antivirus software and notifies the home user if it offers sufficient protection when banking online
	The bank should make timely and frequent public disclosures of information which will assist the public to determine how effective a bank is at risk identification, assessment, monitoring and control.
	General qualitative disclosure requirement Banks must describe their risk management objectives and policies.
Sarbanes-Oxley Act of 2002 (COBIT 4.1)	Banks should identify what home users of online banking need to be made aware of through the ISA programme, such as threats and countermeasure
	Banks should identify home users of online banking as a target audience for user awareness programmes and ensure awareness materials reach all home users of online banking

Legislation	Requirement
	Banks should conduct surveys on security awareness amongst home users of online banking after the implementation of an ISA programme. This should serve as an input for improving the next ISA programme
	Banks should make home users aware of incident reporting procedures and expected response times
	Banks should conduct a survey amongst home users on how satisfied they are with the response to reported online banking incidents. The results should be used to improve the incident response procedure. Home users of online banking should be made aware of new incident reporting procedures and incident response times
Gramm-Leach-Bliley Act of 1999	Banks should make online banking customers aware of the bank's stance on privacy of customers' non-public, personal information.
	Banks should implement an information security plan and standards to protect the security and privacy of customer information, to protect the integrity of customer information from threats and to protect customer information from unauthorised access. This security plan should include an awareness programme aimed at customers of online banking, informing them of the threats relevant to them and countermeasures they may implement to protect themselves.
	Banks should make customers aware of the circumstances under which their non-public, personal information will be shared, how they will be notified and their opt-out options.
	Banks should make customers aware of their privacy policy, dealing with disclosure and protection of customers' non-public personal information. This should be done upon initiation of the customer relationship and annually thereafter until the relationship is terminated.
	Banks should make customers aware of: • The types of organisations their non-public personal information will be shared with • The bank's policy on disclosing current customers' non-public personal information with past customers • The types of customers' non-public personal information collected by the bank • The banks' policy on how it protects the security and confidentiality of customers' non-public personal information

Legislation	Requirement
	Banks should make online banking customers aware of the methods used in pretexting, how to identify pretexting and how to respond. For example, make online banking customers aware of the procedure to be followed when reporting a security incident such as a social engineering or phishing attempt.
Protection of Personal Information Bill Promotion of Access to Information Act, 2000	Not applicable to this research
	Banks should make the home users of online banking aware that only necessary personal information will be collected and processed in a lawful manner, with the consent of the home user
	Banks should make the home users of online banking aware that their personal information will only be collected and processed for legitimate purposes and retained only for as long as required by these purposes. The purposes for collection and processing should be explained to the home user before such collection or processing takes place
	Banks should make the home users of online banking aware that they will be notified and their consent sought should the bank need to process their personal information for purposes not already specified
	Banks should make the home users of online banking aware that their personal information will be kept accurate and up-to-date
	Banks should make the home users of online banking aware that they will always be notified of the types of personal information collected about them and the purpose for which it is being collected and processed
	• Banks should make the home users of online banking aware of the efforts made by the banks to keep personal information safe from loss, unauthorised access and either unlawful processing or disclosure • Banks should also make home users aware of the countermeasures they may implement in order to protect their personal information • Banks should make the home users of online banking aware that they will be notified if it has been established that their personal information has been compromised
	Banks should make home users aware that they are entitled to confirm what personal information is held for the purpose of online banking as well as update or delete, or request to be updated or deleted, personal information held by the bank for the purpose of online banking

Legislation	Requirement
	Banks should make the home users of online banking aware that banks will not unreasonably disclose the home user's personal or financial information in answer to any requestor other than that of the home user
	Banks should make the home users of online banking aware that they will be informed should a requestor, other than the home user, attempt to access either their personal information or their financial information. Banks should also inform home users of their rights to refuse access to their personal information by a requestor
The Code of Banking Practice	Banks should inform personal clients using online banking that they review their bank statements and reconcile their accounts on a regular basis
	Banks should recommend to personal clients using online banking never to reveal their online banking password or any unique, personally identifiable information, even to bank staff
	Banks should recommend to personal clients using online banking that they always check the online banking site's security certificate before carrying out their banking
	Banks should recommend to personal clients using online banking that they change a temporary password to a strong password known to the personal client only as soon as possible
	Banks should recommend to personal clients using online banking that they change their password immediately when they suspect its confidentiality has been compromised
	Banks should make personal clients using online banking aware that the security of their personal computers is the responsibility of the personal client
	Banks should recommend to personal clients using online banking that they read and understand the terms and conditions associated with the online banking service before signing up for the service
	Banks should recommend to personal clients using online banking that they take care to enter login and transaction information accurately
	Banks should recommend to personal clients using online banking that they take care to enter accurate transaction information as it is not possible to reverse transactions without the recipient's consent
	Banks should recommend to personal clients using online banking that they disable "remember my password" browser functionality
	Banks should recommend to personal clients using online banking that they install effective antivirus and security software on their personal computers and that they keep this software up to date

Legislation	Requirement
Consumer Protection Act, 2008	Banks should make consumers aware, in simple, unambiguous language, of any risk associated with the online banking service that a generally alert consumer would not expect
	Banks should make consumers aware of incident reporting facilities and procedures
Constitution of the Republic of South Africa, 1996	Banks should make the home users of online banking aware both of the existence of threats to the privacy of their non-public, personal information and also of the countermeasures they should implement in order to protect the privacy of their non-public, personal information
Code of Governance Principles for South Africa (King III), 25 February, 2009	Banks should make the home users of online banking aware that the banks adopt an uncompromising position regarding the security of online banking transactions
	Banks should make the home users of online banking aware of the threats they face when conducting online banking and also recommend countermeasures which home users should implement to mitigate the associated risks
Electronic Communications Act, 2005	Banks should promote a culture of cybersecurity by developing and implementing ISA programmes aimed at the home users of online banking

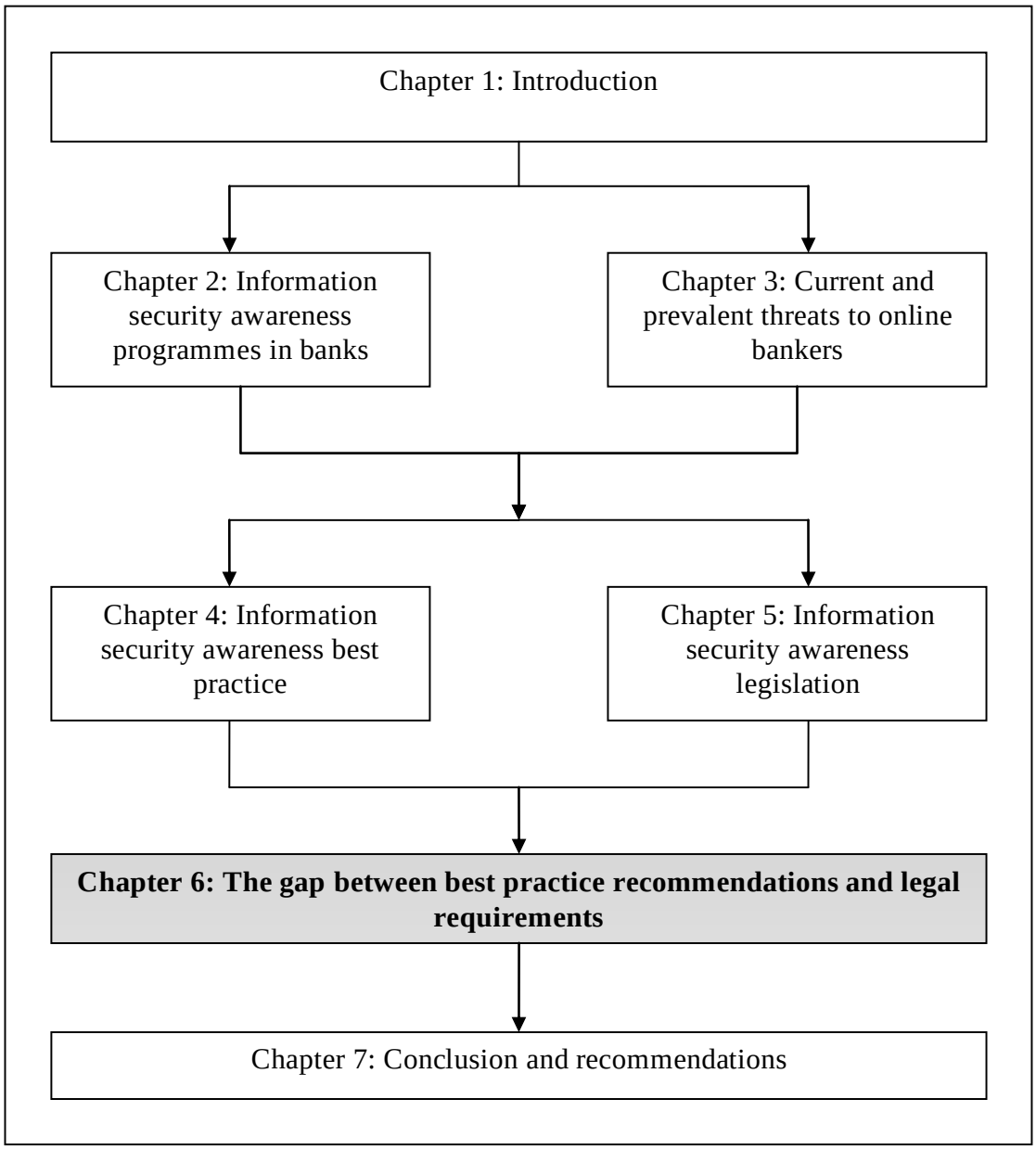
5.5 Summary

In this chapter, a list of laws, regulations, statutes and contractual obligations was selected and analysed for the legal requirements imposed on South African banks regarding ISA programmes aimed at the home users of online banking. Despite the fact that this list is not exhaustive it is deemed sufficient for the purposes of this research. Both international and South African legal documents were analysed. South African banks would need to evaluate their business activities in order to determine which legal requirements pertain to them. Each legal document selected was examined so as to gain an understanding of what an ISA programme would need to include to satisfy the legal requirements. The final outcome of the process is a list of legal requirements to be taken into account when devising such a programme.

In Chapter 6 this list is compared to the final list of best practice recommendations identified in Chapter 4 in order to identify any gaps which exist between best practice recommendations and legal requirements in terms of an ISA programme aimed at the home users of online banking.

Chapter 6:

The Gap between Best Practice Recommendations and Legal Requirements


Chapter 1: Introduction
Chapter 2: Information security awareness programmes in banks
Chapter 3: Current and prevalent threats to online bankers
Chapter 4: Information security awareness best practice
Chapter 5: Information security awareness legislation
Chapter 6: The gap between best practice recommendations and legal requirements
Chapter 7: Conclusion and recommendations

6.1 Introduction

There is a close link between best practice and legislation. Information security best practices address laws and regulations and recommend controls to be implemented to enable organisations to comply with information security legislation. Chapter 4 identified best practice recommendations for information security awareness (ISA) while Chapter 5 identified the ISA requirements imposed on banks by legislation. This chapter compares the best practice recommendations selected and legal requirements selected to determine whether compliance with best practices would result in compliance with legislation.

6.2 Comparison of Legal Requirements and Best Practice Recommendations

The main objective of this research study is a comparison between best practice recommendations and the legal requirements for information security awareness. The gap identified between best practice recommendations and the legal requirements is the main outcome of this research study and comprises the contribution made by this study to the area of research. In Chapter 4, selected best practices, which are internationally recognised and implementable in banks, were analysed for recommendations when implementing an ISA programme aimed at the home users of online banking. A similar analysis was conducted in Chapter 5 but with the focus on selected legislation pertinent to South African banks and with information security implications. The best practice recommendations identified include the following:

A. Banks should identify what the home users of online banking need to be made aware of through the medium of ISA programmes, for example, threats and countermeasures.
B. Banks should identify the home users of online banking as a target audience for user awareness programmes and ensure that awareness materials reach all the home users of online banking.
C. Banks should conduct surveys on the level of security awareness amongst the home users of online banking after the implementation of an ISA programme. These results should serve as an input for improving the next ISA programme.

D. Banks should make home users aware of incident-reporting procedures and expected response times.
E. Banks should conduct a survey amongst home users on their level of satisfaction with the response to online banking incidents reported. These results should be used to improve the incident response procedure. Home users of online banking should then be made aware of new incident reporting procedures and incident response times.
F. Banks should make the home users of online banking aware of ways in which they may protect their information.
G. Banks should make home users aware of, and require them to comply with, certain security requirements as stipulated in the information security policy before signing up for online banking.
H. Banks should demonstrate to the home users of online banking that the banks adopt an uncompromising position in respect of information security management and awareness.

The legal requirements identified include the following:

1. Banks should identify home users of online banking as a target audience for user awareness programmes and ensure awareness materials reach all home users of online banking.
2. Banks should make consumers aware, in plain language, of any risk associated with the online banking service that an ordinarily alert consumer would not expect.
3. Banks should promote a culture of cybersecurity by developing and implementing an ISA programme aimed at home users of online banking.
4. Banks should make home users of online banking aware that they take a stern stance on the security of online banking transactions and privacy of personal information.
5. The bank should make timely and frequent public disclosures of information which will assist the public to determine how effective a bank is at risk identification, assessment, monitoring and control. This should include the use of an independent auditor.

6. Banks should make home users of online banking aware of the threats they face when online banking, including threats to the privacy of their personal information, and recommend countermeasures they should implement to mitigate the associated risks.
7. Banks should make antivirus software available to home users of online banking.
8. Banks should make home users aware of incident reporting procedures and expected response times.
9. Banks should review the content of ISA programmes to include new threats, changes in incident reporting procedures and response times and make home users aware of these new threats.
10. Banks should make home users of online banking aware of their privacy policy, dealing with disclosure and protection of customers' non-public personal information. This should be done upon initiation of the customer relationship and annually thereafter until the relationship is terminated.
11. Banks should make home users of online banking aware that their personal information will only be collected and processed for legitimate purposes and retained only for as long as required by these purposes. The purposes for collection and processing should be explained to the home user before collection or processing takes place.
12. Banks should make home users of online banking aware that they will be notified if it can be established that their personal information has been compromised.
13. Banks should make home users aware that they are entitled to confirm what personal information is held for the purpose of online banking as well as update or delete, or request to be updated or deleted, personal information held by the bank for the purpose of online banking.
14. Banks should make home users of online banking aware that they will be informed should a requestor other than the home user attempt to access their personal information or financial information. The bank should also inform the home user of their rights to refuse access to their personal information by the requestor.
15. Banks should recommend to personal clients using online banking that they review their bank statements and reconcile their accounts on a regular basis.

16. Banks should make personal clients using online banking aware that security of their personal computer is the responsibility of the personal client.
17. Banks should recommend to personal clients using online banking that they read and understand the terms and conditions associated with the online banking service before signing up for the service.
18. Banks should recommend to personal clients using online banking that they be careful to enter accurate transaction information as transactions cannot be reversed without the recipient's consent.

Figure 6-1 illustrates the gap between the legal requirements selected and the best practice recommendations selected by showing which best practice recommendations support which legal requirement.

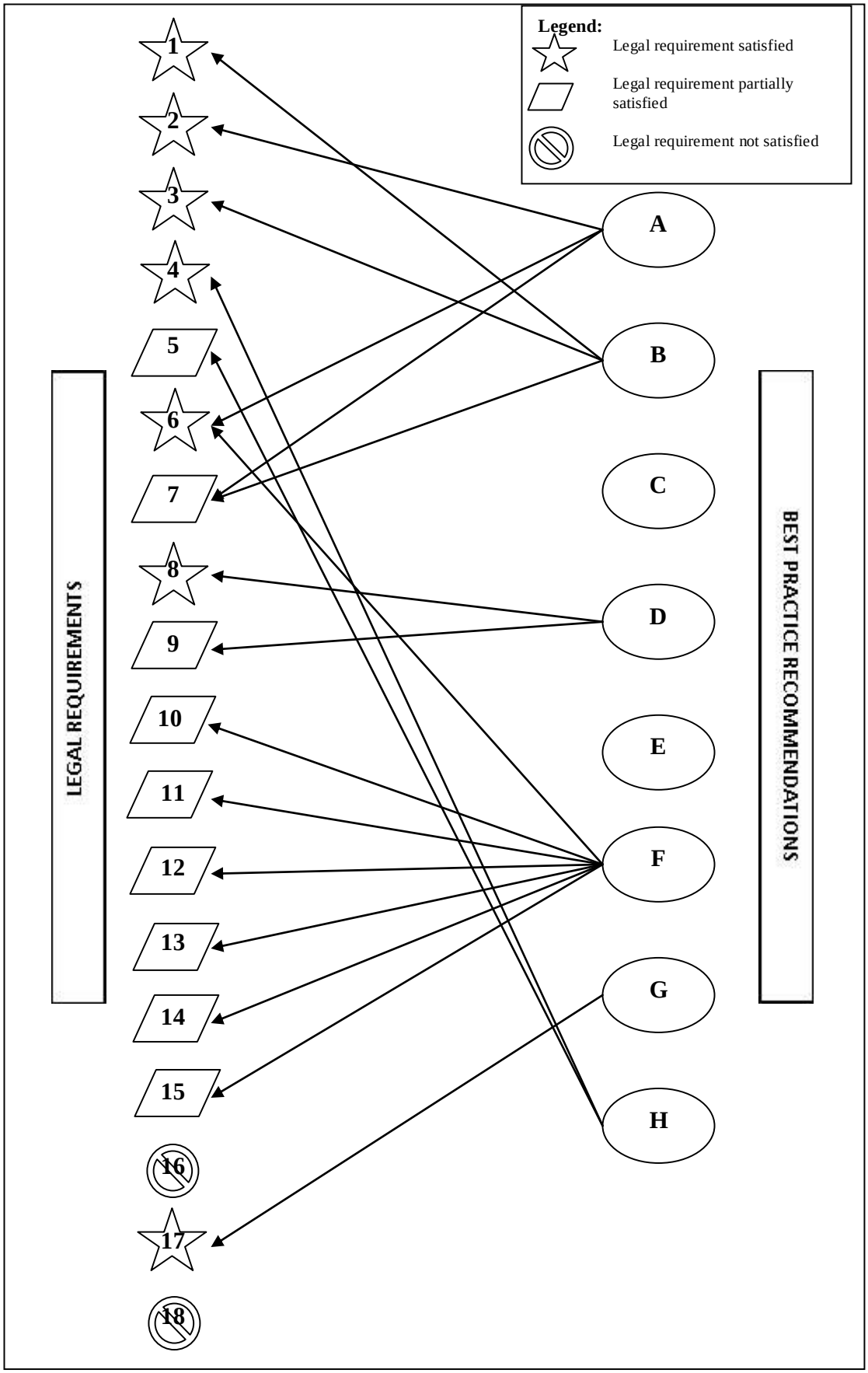


Figure 6-1 Comparison of legal requirements and best practice recommendations

6.3 Findings

Finding 1: The results show that the implementation of the selected best practice recommendations would fully satisfy seven of the 18 legal requirements only and partially satisfy the other nine. There are no other recommendations offered for two of the 18 legal requirements.

Finding 2: Compliance with legal requirements 1 to 4, 6, 8 and 17 may be achieved through the implementation of best practice recommendations.

Finding 3: Legal requirement number 5 is partially satisfied by the selected best practices. Selected best practices require a bank to demonstrate a stern stance on risk management, but do not explicitly require a bank to disclose incidents which would be material to the home users' decisions to continue making use of the online banking service.

Finding 4: Legal requirements number 7 is partially satisfied by the implementation of best practice recommendations. The selected best practice recommendations do not explicitly require banks to make security software available to home users of online banking, as required by legal requirement number 7. However, the selected best practices recommend that banks make home users of online banking aware of countermeasures they can implement and recommend awareness materials reach all home users. Security software may be included in the awareness materials;

Finding 5: Legal requirement number 9 is only partially satisfied by the implementation of selected best practice recommendations. The recommendations do not state the need to update the content of the ISA programme to include new threats. However, the Standard of Good Practice for Information Security statement UE6.2.6 recommends that banks should review security incidents and use findings to update the next ISA programme aimed at home users of online banking. Such a review would reveal previously unidentified threats to home users of online banking.

Finding 6: Although the selected best practices recommend that banks make home users aware of how they can protect their personal information, legal

requirements 10 to 15 suggest that best practices do not offer sufficient guidance on ensuring privacy of personal information. However, the Standard of Good Practice for Information Security section UE6.1 does address information privacy, recommending that banks develop and implement approved methods for handling personally identifiable information.

Finding 7: No matches for legal requirements numbers 16 and 18 suggest that the selected best practices do not stipulate the need for home users to be made aware of what their responsibilities are when protecting themselves.

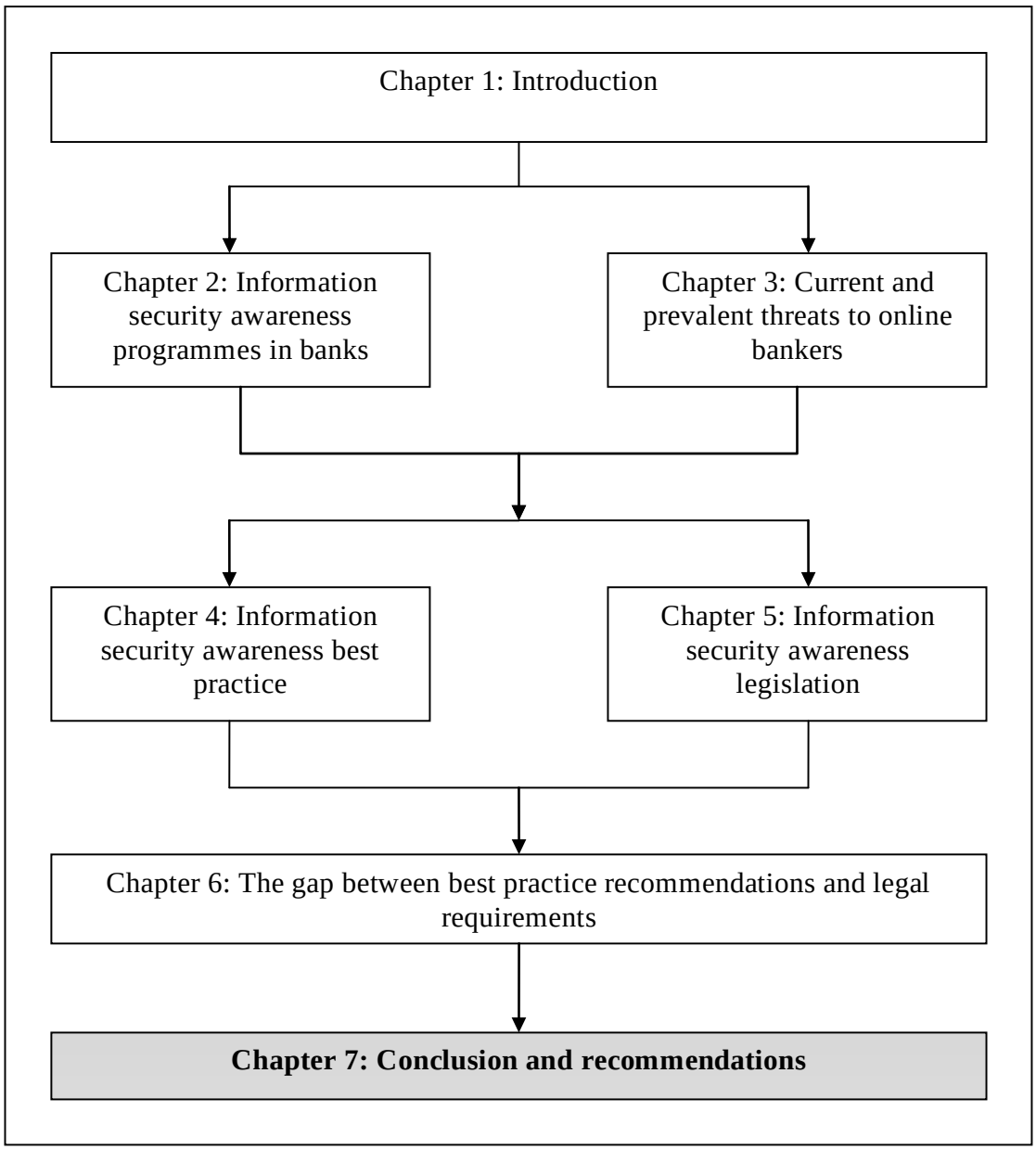
It may, thus, be concluded that implementing the ISA recommendations identified in the selected best practices does not result in compliance with the ISA requirements identified in the selected legislation.

6.4 Summary

In this chapter, the recommendations identified in the selected best practices in Chapter 4 were compared to the requirements identified in the selected legislation in Chapter 5. A gap was identified, which demonstrated that the implementation of the selected best practices does not result in compliance with the requirements identified in the selected legislation. It is essential that banks first be aware of the legislation with which they have to comply and then select controls from reputable best practices and international standards to ensure compliance. However, the best practices and international standards consulted should not be limited to those analysed in this research.

Chapter 7:

Conclusion and Recommendations


Chapter 1: Introduction
Chapter 2: Information security awareness programmes in banks
Chapter 3: Current and prevalent threats to online bankers
Chapter 4: Information security awareness best practice
Chapter 5: Information security awareness legislation
Chapter 6: The gap between best practice recommendations and legal requirements
Chapter 7: Conclusion and recommendations

7.1 Introduction

A large number of South African home users are becoming aware of and are, in turn, able to use online banking. Consequently, these home users of online banking are facing multiple information security threats while conducting their online banking. From a security perspective, it is essential that the human element of the security chain be addressed. Accordingly, the focus of this research has been on home users and the actions which South African banks are both required and advised to take when implementing Information Security Awareness (ISA) programmes aimed at the home users of online banking.

It is vital that South African banks protect their home users from the information security threats they face as online bankers, that they be able to demonstrate due care and due diligence when addressing these information security threats by implementing best practice, and that they recognise and comply with the legal requirements imposed on them.

In this chapter, both the problem statement and the research questions are revisited to confirm the research findings. Related problem areas which have emerged from the research are discussed as well as the way in which these problem areas may be addressed by future work.

7.2 Scope of Research

This research investigated the following three main areas:

- Information security threats facing home users of online banking, creating the need for security initiatives and industry regulation
- Recommendations from selected best practices for the implementation of an ISA programme aimed at home users of online banking
- Requirements from selected legislation placed on South African banks for information security awareness of home users of online banking

The results from a gap analysis compared the recommendations identified from selected information security best practice with the requirements identified from selected information security legislation. The gap identified, the limitations of this research and the nature of information security threats form the basis for further research on the subject.

7.3 Problem Areas identified through the Research

Certain problem areas related to the problem statement emerged from the research. It is essential that these problem areas be attended to in future research into the field of information security in online banking.

7.3.1 The Gap

It was discovered that the implementation of the selected best practice recommendations does not result in compliance with all the selected ISA legal requirements.

7.3.2 Limited Number of Best Practice Standards Included

This research included three international best practice documents and not an exhaustive list of best practice documents. Best practice documents not included in this research could offer guidance in respect of the outstanding legal requirements not satisfied by selected best practice recommendations.

7.3.3 Legislation is Open to Interpretation

Legislation is written in a high-level fashion, can be ambiguous and is therefore open to interpretation. For this reason, other researchers may gather findings which differ from those gathered in this research.

7.3.4 The Provision for Evolving Threats in Legislation

Hackers are constantly evolving their attack methods. Laws and regulations may not advance fast enough to effectively address new information security threats.

7.3.5 Validation of Research Findings

This research investigated the requirements imposed on South African banks, but did not investigate the relevance of the findings to South African banks. The research does not determine if a gap exists between ISA best practice implemented by a South African bank and the legislation they are required to comply with.

7.4 Research Questions

This section re-visits the research questions as depicted in Chapter 1.

7.4.1 Information Security Best Practice

The first research question set out to determine information security best practice recommendations for information security awareness of home users of online banking. Information security best practice documents were selected based on the criteria that they are internationally recognised, implementable in a banking environment and are available to the public. The best practices identified included COBIT version 4.1, ISO/IEC 27001 and The Standard of Good Practice for Information Security. Each selected document was analysed for the guidance it offers for the implementation of an ISA programme. The result was a final list of eight best practice recommendations for information security awareness.

7.4.2 Information Security Legislation

The second research question set out to determine the information security legal requirements imposed on South African banks regarding information security awareness of their home users of online banking. An information security attorney and privacy professional from Deloitte and Touche was consulted for their opinion on which legal documents to include. They recommended international banking legislation and South African legislation and also suggested other relevant documents. In addition, a visit to the South African government's website for publicly available documents was also carried out to research other pertinent documents and to identify

relevant amendments to the final list of documents. Each selected legal document was analysed for the requirements imposed on South African banks when implementing an ISA programme aimed at the home users of online banking. The result was a list of 18 legal requirements for information security awareness.

7.4.3 Identifying the Gap

The third research question set out to identify any gap between ISA best practice recommendations and existing ISA legal requirements. The best practice recommendations identified from selected best practice documents in Chapter 4 were compared to the legal requirements identified in selected legislation in Chapter 5 and a gap was, indeed, noted.

7.4.4 The Problem Statement

The following problem statement forms the core of this research as depicted in Chapter 1:

If South African banks implement information security awareness best practices, do they automatically comply with information security awareness laws and regulations?

The findings of this research indicate that the implementation of the selected best practices included in this research does not result in compliance with the legal requirements identified in the legislation selected for this research.

7.5 Future Work

The comparison between the identified recommendations from selected best practices and the identified requirements from selected legislation determined that there is, indeed, a gap between the recommendations and the requirements. Further research could determine the reason why this gap exists. The list of best practices analysed in this research was not exhaustive and, thus, further research could be carried out to

determine whether other best practice documents include recommendations which may satisfy the gaps identified. In view of the fact that the legal documents included in this research are written in a high-level fashion and may be ambiguous they may, thus, be open to interpretation. Accordingly, further research into legal requirements is recommended to uncover new findings and to offer new insights into what these documents aim to achieve and how organisations may comply with these requirements. Further research may also be conducted to determine whether the legislation is advancing in such a way so that guidance is offered on the ever-evolving attack methods used by hackers. Finally, although this research did extract the requirements imposed on South African banks, it did not investigate the relevance of the findings to South African banks. A case study carried out at a South African bank may determine whether the bank is aware of all the ISA legal requirements imposed on banks and what best practice controls the bank has in place to satisfy these requirements.

7.6 Summary

A large number of South African home users are becoming aware of and are, thus, able to use online banking. Consequently, these home users of online banking are facing multiple information security threats while conducting their online banking. From a security perspective, it is essential that the human element of the security chain be addressed. Accordingly, the focus of this research has been on home users and the actions South African banks are both required and advised to take when implementing ISA programmes aimed at the home users of online banking.

In this chapter, the problem statement and research questions were revisited to confirm the validity of the method used and the research findings. Related problem areas which emerged from the research were discussed as well as the way in which these problem areas may be addressed by future work.

The problem areas which emerged from this research focused on the following:

- the existence of a gap between selected best practice recommendations and selected legal requirements
- the inclusion of a larger number of best practice documents researched

- the ambiguity of legislation and the possibility of different interpretations and findings on the part of different researchers
- whether legislation is advancing in such a way that it is addressing the ever-evolving information security threats

These problem areas may form the foundation for future work in the area of online banking security.

The primary outcome of this research was a comparison between identified best practice recommendations and identified legal requirements to determine whether a gap existed between them. The findings of the research indicate that the implementation of the selected best practices included in this research does not result in compliance with the legal requirements identified in the legislation selected for this research.

References used in text

Adviza Consultants 2009, "A Whitepaper ISO27001: Overview and benefits".

Ahmad, M.K.A., Rosalim, R.V., Yu Beng, L. & Soo Fun, T. 2010, "Security issues on banking systems", International Journal of Computer Science and Information Technologies, vol. 1, no. 4, pp. 268–278.

Albrechtsen, E. 2007, "A qualitative study of users' views on information security", Computers & Security, vol. 26, no. 4, pp. 276–289.

Albrechtsen, E. & Hovden, J. 2009, "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study." Computers & Security, vol. In Press, no. Corrected proof.

Al-Somali, S.A., Gholami, B. & Clegg, B. 2009, "An investigation into the accpetance of online banking in Saudi Arabia", Technovation, vol. 29, no. 2, pp. 130–141.

Anderson, J.M. 2003, "Why we need a new definition of Information Security", Elsevier, pp. 308–313.

Ashley, P., Hinton, H., Vandenwauver, M. & IBM Software Group 2001, "Wired versus Wireless Security: The Internet, WAP and iMode for E-Commerce", Computer Security Applications Conference, 2001. ACSAC, 2001. Proceedings 17th AnnualIEEE Xplore Digital Library, USA.

Banking Information Security 2011, 2011-last update [Homepage of ISMG Corp], [Online]. Available: www.bankinfosecurity.com.

Basel Committee on Banking Supervision 2004, Basel II, Bank for International Settlements, Switzerland.

Basel Committee on Banking Supervision 2003, Sound Practices for the Management and Supervision of Operational Risk, Bank for International Settlements, Switzerland.

Birch, G. 1999, "Mobile financial services: The Internet isn't the only digital channel to consumers", Journal of Internet Banking and Commerce, vol. 4, no. 1.

Blumstein, A. 1978, "Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates", National Academy of Sciences.

Bose, I. & Leung, A.C.M. 2008, "Assessing anti-phishing preparedness: A study of online banks in Hong Kong", Decision Support Systems, vol. 45, no. 4, pp. 897–912.

Brenner, S.W. 2007, "History of Computer Crime" in The History of Information Security: A Comprehensive Handbook, eds. K. de Leeuw & J. Bergstra, Elsevier BV, USA, pp. 705–721.

British Standards Institution 2005, BS ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements, 2005th edn, British Standards Publishing Limited.

Brown, I., Cajee, Z., Davies, D. & Stroebel, S. 2003, "Cell phone banking: predictors of adoption in South Africa – an exploratory study", International Journal of Information Management, vol. 23, no. 5, pp. 381–394.

BusinessDictionary 2011, 2011–last update, BusinessDictionary [Homepage of WebFinance, Inc], [Online]. Available: http://www.businessdictionary.com/definition/best-practice.html [2011, 03/31].

Calder, A. 2009, Information security based on ISO 27001/ISO 17799: A Management Guide, Van Haren Publishing.

Cambridge Dictionaries Online 2011[a], 2011–last update [Homepage of Cambridge University Press], [Online]. Available: http://dictionary.cambridge.org/dictionary/british/law_1 [2011, 01/12].

Cambridge Dictionaries Online 2011[b], 2011–last update [Homepage of Cambridge University Press], [Online]. Available: http://dictionary.cambridge.org/dictionary/british/regulation_1 [2011, 01/12].

Cambridge Dictionaries Online 2011[c], 2011–last update [Homepage of Cambridge University Press], [Online]. Available: http://dictionary.cambridge.org/dictionary/british/statute [2011, 01/12].

Campbell, J., Greenauer, N., Macaluso, K. & End, C. 2007, "Unrealistic optimism in internet events", Computers in Human Behaviour, vol. 23, no. 3, pp. 1273–1284.

CIO.com2011, 2011–last update [Homepage of CXO Media Inc], [Online]. Available: www.cio.com [2010, 06/07].

Cline, M. & Jensen, B. 2004, "Information Security: an organisational change perspective", AMCIS 2004 Proceedings USA.

Constitution of the Republic of South Africa No. 108 of 1996 1996, , South Africa, South Africa.

Consumer Protection Act, 2008 2008, , Act edn, South Africa, South Africa.

Cranor, L.F. 2008, "A framework for reasoning about the human in the loop", UPSEC '08 Proceedings of the 1st Conference on Usability, Psychology, and SecurityUSENIX Association, USA.

CSO Online – Security and Risk2011, 2011–last update [Homepage of CXO Media Inc], [Online]. Available: www.csoonline.com [2010, 06/07].

Da Veiga, A. & Eloff, J.H.P. 2010, "A framework and assessment instrument for information security culture", Computers & Security, vol. 29, no. 2, pp. 196–207.

Dahdah, H. 2008, Phishing scam mimics NSW fraud squad to snare victims, IDG Communications, http://www.computerworld.com.au/article/214141/phishing_scam_mimics_nsw_fraud_squad_snare_victims/.

Desman, M.B. 2002, Building an Information Security Awareness Program, First edn, CRC Press LLC, Boca Raton.

Dhamija, R., Tygar, J.D. & Hearst, M. 2006, "Why phishing works", Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM Press, New York.

Dodge, R.C., Carver, C. & Ferguson, A.J. 2007, "Phishing for user security awareness", Computers & Security, vol. 26, no. 1, pp. 73–80.

Donchez, T. 2008, Internet Safety: The Basics, ISMG Corp, http://www.bankinfosecurity.com/articles.php?art_id=730&search_keyword=donchez&search_method=exact.

Draft Cybersecurity Policy of South Africa 2010, Draft Policy edn, South Africa, South Africa

Electronic Communications Act No. 36 of 2005 2006, Act edn, South Africa, South Africa.

Electronic Communications and Transactions Act, 2002 2002, Act edn, South Africa, South Africa.

"Elsevier Journals", 2011, Elsevier [Online]

ENISA 2006, A users' guide: how to raise information security awareness, European Network and Information Security Agency.

Field, T. 2010[a], 2010-last update, Marketing security as a competitive edge: interview with author Joseph Menn on fighting banking frauda [Homepage of ISMG Corp], [Online]. Available: http://www.bankinfosecurity.com/articles.php?art_id=2614 [2010, 06/07].

Field, T. 2010[b], Banking malware: end users are 'Achilles Heel'b, ISMG Corp, http://www.bankinfosecurity.com/articles.php?art_id=2840.

Field, T. 2009, Gartner's John Pescatore on 2010 Threats, Trendsc, ISMG Corp, http://careers.testinfosecurity.com/articles.php?art_id=1926.

Furnell, S.M. 2008, "End-user security culture: a lesson that will never be learnt?", Computer Fraud & Security, vol. 2008, no. 4, pp. 6–9.

Furnell, S.M. 2005, "Why users cannot use security", ScienceDirect, vol. 24, no. 4, pp. 274–279.

Furnell, S.M., Tsaganidi, V. & Phippen, A. 2008, "Security beliefs and barriers for novice internet users", Computers & Security, vol. 27, no. 7–8, pp. 235–240.

Galup, S.D., Dattero, R., Quan, J.J. & Conger, S. 2009, "An overview of IT service management", Communications of the ACM, vol. 52, no. 5.

Gerber, M. & von Solms, R. 2008, "Information security requirements: interpreting the legal aspects", Computers & Security, vol. 27, no. 5–6, pp. 124–135. \

Gikandi, J.W. & Bloor, C. 2009, "Adoption and effectiveness of electronic banking in Kenya", Electronic Commerce Research and Applications, vol. In Press, no. Corrected Proof.

Goodchild, J. 2010[a], Social Engineering: The Basics, CXO Media, Inc, http://www.csoonline.com/article/514063/social-engineering-the-basics.

Goodchild, J. 2010[b], ACH Fraud: Why criminals love this con, CXO Media, Inc, http://www.csoonline.com/article/603461/ach-fraud-why-criminals-love-this-con.

Gramm-Leach-Bliley Act of 1999 1999, Act edn, International.

Granova, A. & Eloff, J.H.P. 2005, "A legal overview of phishing", Computer Fraud & Security, vol. 2005, no. 7, pp. 6–11.

Hansche, S. 2001, "Designing a security awareness program: part 1", Information Systems Security, vol. 9, no. 6, pp. 14–22.

Hardy, G. 2006, "Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges", Information Security Technical Report, vol. 11, no. 1, pp. 55–61.

Harris, S. 2008, All-in-One CISSP Exam Guide, 4th edn, McGraw-Hill Osborne Media, USA.

Höne, K. & Eloff, J.H.P. 2002, "Information security policy: what do international information security standards say?", Computers & Security, vol. 21, no. 5, pp. 402–409.

Humphreys, T. 2006, "State-of-the-art information security management systems with ISO/IEC 27001:2005", ISO Management Systems, no. January–February.

Hwang, V. 2008, Tis' the season for online shopping and holiday e-threats, CXO Media, Inc, http://www.cio.com/article/472364/Tis_the_Season_for_Online_Shopping_and_Holiday_E_Threats?page=2&taxonomyId=3169.

Information Security Forum 2007, The Standard of Good Practice for Information Security, ISF, USA.

Investorwords 2011, 2011-last update, Investorwords [Homepage of WebFinance, Inc], [Online]. Available: http://www.investorwords.com/3420/online_banking.html [2010, 07/06].

ISO 27000 Directory, ISO 27000 - ISO 27001 and ISO 27002 Standards2009, 2009- last update [Homepage of ISO 27000 Directory], [Online]. Available: http://www.27000.org/ [2010, 11/11].

IT Governance Institute 2007, COBIT 4.1, ITGI, USA.

Johansson, E. & Johnson, P. 2005, "Assessment of enterprise information security: an architecture theory diagram definition", Conference on Systems Engineering ResearchStevens Institute of Technology, USA, pp. 136.

Kelly, C.J. 2006, "Awareness trumps new security toys", Computerworld, vol. 40, no. 41, pp. 44–44.

Kim, C., Tao, W., Shin, N. & Kim, K. 2010, "An empirical study of customers' perceptions of security and trust in e-payment systems", Electronic Commerce Research and Applications, vol. 9, no. 1, pp. 84–95.

King Committee on Governance 2009, Code of Governance Principles for South Africa (King III), Institute of Directors in Southern Africa, South Africa.

Kordel, L. 2004, "IT governance hands-on: using COBIT to implement IT governance", Information Systems Control Journal, vol. 2.

Kruger, H.A. & Kearney, W.D. 2008, "Consensus ranking: an ICT security awareness case study", Computers & Security, vol. 27, no. 7–8, pp. 254–259.

Kruger, H.A. & Kearney, W.D. 2006, "A prototype for assessing information security awareness", Computers & Security, vol. 25, no. 4, pp. 289–296.

Lainhart, J.W. 2000, "COBIT: A methodology for managing and controlling information and information technology risks and vulnerabilities", Journal of Information Systems, vol. 14, no. 1.

Lassar, W.M., Manolis, C. & Lassar, S.S. 2005, "The relationship between consumer innovativeness, personal characteristics, and online banking adoption", International Journal of Bank Marketing, vol. 23, no. 2, pp. 176–199.

Laukkanen, T., Sinkkonen, S. & Laukkanen, P. 2009, "Communications strategies to overcome functional and psychological resistance to Internet banking", International Journal of Information Management, vol. 29, no. 2, pp. 111–118.

Loermans, J. 2002, "Synergising the learning organization and knowledge management", Journal of Knowledge Management, vol. 6, no. 3, pp. 285–294.

May, C. 2008, "Approaches to user education", Network Security, vol. 2008, no. 9, pp. 15–17.

McGlasson, L. 2010[a], Texas bank sues customer after $800 000 scam, Bankinfosecurity.com, U.S.A.

McGlasson, L. 2010[b], 2009 Data breaches: an interactive timelineb, ISMG Corp, http://www.bankinfosecurity.com/articles.php?art_id=1766&opg=1.

McKenna, B. 2009, "Awareness training 2.0", Infosecurity, vol. 6, no. 7, pp. 18-20.

McMillan, R. 2009, Citing cybercrime, FBI Director doesn't bank online, IDG Communications, http://www.techworld.com.au/article/321410/citing_cybercrime_fbi_director_doesn_t_bank_online/.

Methods & Tools QA Resources 2009, 2009–last update [Homepage of Quality Assurance Project], [Online]. Available: http://www.qaproject.org/methods/resglossary.html [2010, 11/11].

Moringiello, J.M. 2010, "Warranting data security", Brooklyn Journal of Corporate, Financial & Commercial Law, vol. 5.

Neale, F.R. & Peterson, P.P. 2005, "The effect of the Gramm-Leach-Bliley Act on the insurance industry", Journal of Economics and Business, vol. 57, pp. 317–338.

Oxford English Dictionary 2011[a], 2011–last update [Homepage of Oxford University Press], [Online]. Available: http://www.oed.com/view/Entry/106405?rskey=dlvFL7&result=1&isAdvanced=false#eid [2011, 01/12].

Oxford English Dictionary 2011[b], 2011–last update [Homepage of Oxford University Press], [Online]. Available: http://www.oed.com/view/Entry/264317?redirectedFrom=phishing#eid [2011, 01/12].

Oxford English Dictionary 2011[c], 2011–last update, Oxford English Dictionary [Homepage of Oxford University Press], [Online]. Available: http://www.oed.com/view/Entry/161427?redirectedFrom=regulation#eid [2011, 01/12].

Oxford English Dictionary 2011[d], 2011–last update, Oxford English Dictionary [Homepage of Oxford University Press], [Online]. Available: http://www.oed.com/search?searchType=dictionary&q=statute&_searchBtn=Search [2011, 01/12].

Peltier, T.R. 2005, "Implementing an information security awareness program", EDPACS, vol. 33, no. 1, pp. 1–18.

Pikkarainen, T., Pikkarainen, K., Karjaluoto, H. & Pahnila, S. 2004, "Consumer acceptance of online banking: an extension of the technology acceptance model", Internet Research, vol. 14, no. 3, pp. 224–235.

Porteous, D. 2006, The enabling environment for mobile banking in Africa, Department for International Development, USA.

Potter, B. 2009, "High time for trusted computing", Security & Privacy, IEEE, vol. 7, no. 6, pp. 54–56.

Promotion of Access to Information Act, 2000 2000, Act edn, South Africa, South Africa.

Protection of Personal Information Bill, 2009 2009, Bill edn, South Africa.

Rasiah, D. 2010, "ATM Risk Management and Controls", European Journal of Economics, Finance and Administrative Sciences, no. 21, pp. 161–171.

Richardson, R.D., CSI 2008, "CSI computer crime and security survey", Computer Security Institute, pp. 2008–2008.

Ridley, G., Young, J. & Carroll, P. 2004, "COBIT and its utilization: A framework from the literature.",Proceedings of the 37th Hawaii International Conference on System Sciences.

Rotvold, G. 2008, "How to create a security culture in your organisation", Information Management Journal, vol. 42, no. 6, pp. 32–38.

RSA 2007, No time for declarations of victory: Protecting customers beyond compliance deadlines, RSA Security Inc, USA.

Sadique Sohail, M. & Shanmugham, B. 2003, "E-banking and customer preferences in Malaysia: An empirical investigation", Information Sciences, vol. 150, no. 3–4, pp. 207–217.

SafeNet 2010, Top online banking threats to financial service providers in 2010, SafeNet.

SafeNet 2009, Confidence in commernce: enabling e-banking and online serviceswith two-factor authentication, SafeNet.

SANS: Computer Security Training, Network Security Research, InfoSec Resources2011, 2011–last update [Homepage of The SANS Institute], [Online]. Available: www.sans.org [2010, 06/07].

Sathye, M. 1999, "Adoption of Internet banking by Australian consumers: an empirical investigation", International Journal of Bank Marketing, vol. 17, no. 7, pp. 324–334.

Siponen, M.T. 2000, "A conceptual foundation for organizational information security awareness", Information Management and Computer Security, vol. 8, no. 1, pp. 31-41.

Siponen, M.T. 2001, "Five dimensions of information security awareness", ACM SIGCAS computers and society, vol. 31, no. 2, pp. 24-29.

Siponen, M. 2006, "Information security standards focus on the existence of process, not its content", Communications of the ACM, vol. 49, no. 8, pp. 97-100.

Smith, H.A. & McKeen, J.D. 2003, "The Evolution of the KM function", [Online], pp. 02/02/2011. Available from: https://business.queensu.ca/knowledge/workingpapers/working/working_03-07.pdf.

South Africa Internet Usage and Marketing Report2009, 2009–last update [Homepage of Miniwatts Marketing Group], [Online]. Available: http://www.internetworldstats.com/af/za.htm [2010, 07/06].

SOX-Online: The Vendor-Neutral Sarbanes-Oxley Site2009, 2009–last update. Available: http://www.sox-online.com/ [2010, 11/25].

Spremic, M. & Popovic, M. 2008, "Emerging issues in IT governance: implementing the corporate risks IT management model", WSEAS TRANSACTIONS on SYSTEMS, vol. 7, no. 3.

Spring, T. 2007, How to Avoid Being a Phishing Scam Victim, CXO Media, Inc, http://www.cio.com/article/106001/How_to_Avoid_Being_a_Phishing_Scam_Victim

Swart, R. 2007, Transcript of Betsy Broder of FTC on identity protection strategies, ISMG Corp, http://www.bankinfosecurity.com/articles.php?art_id=629.

Symantec 2007, Symantec Internet Security Threat Report: September 2007 Financial Services Industry Data Sheet, Symantec, USA.

Taylor, L. & Shepherd, M. 2007, "Addressing security awareness and training requirements" in FISMA certification and accreditation handbook, eds. M. Shepherd & A. Rebello, 2007th edn, Syngress Publishing Inc., USA., pp. 139–148.

The Anti-Phishing Working Group 2009, Phishing activity trends report 1st half 2009, APWG, USA.

The Banking Council, South Africa 2004, Code of Banking Practice, The Banking Council, South Africa, South Africa.

The Institute of Internal Auditors 2008, Sarbanes-Oxley Section 404: a guide for management by internal controls practitioners, 2nd edn, The Institute of Internal Auditors.

The National Cybersecurity Alliance 2010, 2010-last update, Stay Safe Online [Homepage of StaySafeOnline – NCSA], [Online]. Available: http://www.staysafeonline.org [2010, 06/07].

The National Cybersecurity Alliance 2010, What home users can do, National Cybersecurity Awareness Alliance, USA.

Ugochuku, I. 2006, SOX 404 & IT Controls: IT Control Recommendations for Small and Mid-size Companies, TLK Enterprise.

Valentine, J.A. 2006, "Enhancing the employee security awareness model", Computer Fraud & Security, vol. 2006, no. 6, pp. 17–19.

Verisign 2008, A guide to providing proactice protection to consumer online transactions, Verisign Inc, U.S.A.

Verisign 2007, It's a matter of trust: when the customer relationship is everything, business bank on SSL solutions, Bankinfosecurity (ISMG Media Group).

von Solms, B. 2005, "Information security governance: COBIT or ISO 17799 or both?" Computers & Security, vol. 24, no. 2, pp. 99–104.

von Solms, B. & von Solms, R. 2004, "The 10 deadly sins of information security management", Computers & Security, vol. 23, no. 5, pp. 371–376.

Weil, N. 2008, Top 10 IT News Stories of the Week - Another New Trojan Intercepts Online Banking Information, CXO Media, Inc, http://www.cio.com/article/173700/Top_10_IT_News_Stories_of_the_Week.

West, R. 2008, "The psychology of security", Communications of the ACM, vol. 51, no. 4.

Wiederkehr, B. 2003, "IT Security Awareness Programme", Information Systems Control Journal, vol. 3.

Wikipedia 2011[a], 17/02/2011–last update, [Homepage of WikiMedia Foundation, Inc], [Online]. Available: http://en.wikipedia.org/wiki/Online_banking [2010, 07/06].

Wikipedia 2011[b], 17/02/2011–last update, [Homepage of Wikimedia Foundation, Inc], [Online]. Available: http://en.wikipedia.org/wiki/Best_practice [2010, 11/11].

Wikipedia 2011[c], 17/02/2011–last update, [Homepage of WikiMedia Foundation, Inc], [Online]. Available: http://en.wikipedia.org/wiki/Phishing [2010, 07/06].

Wikipedia 2011[d], 17/02/2011–last update, [Homepage of WikiMedia Foundation, Inc], [Online]. Available: http://en.wikipedia.org/wiki/Social_engineering_(security) [2011, 03/15].

Wikipedia 2011[e], 17/02/2011–last update, [Homepage of WikiMedia Foundation, Inc], [Online]. Available: http://en.wikipedia.org/wiki/Malware [2011, 03/15].

Wikipedia 2011[f], 17/02/2011–last update, [Homepage of WikiMedia Foundation, Inc], [Online]. Available: http://en.wikipedia.org/wiki/Encryption [2011, 03/15].

Wikipedia 2011[g], 17/02/2011–last update, [Homepage of WikiMedia Foundation, Inc], [Online]. Available: http://en.wikipedia.org/wiki/Firewall_(computing) [2011, 03/15].

Wikipedia 2011[h], 17/02/2011–last update, [Homepage of WikiMedia Foundation, Inc], [Online]. Available: http://en.wikipedia.org/wiki/Antivirus [2011, 03/15].

Wikipedia 2011[i], 17/02/2011–last update, [Homepage of WikiMedia Foundation, Inc], [Online]. Available: http://en.wikipedia.org/wiki/Identity_theft [2011, 03/15].

Wiles, J., Claypoole, T., Henry, P.A., Drake, P., Lowther, S., 2008, "Developing an effective security awareness program", Techno Security's Guide to Securing SCADA, vol. 13, no. 4, pp. 137–169.

Williams, P.A.H. 2008, "In a 'trusting' environment, everyone is responsible for information security", Information Security Technical Report, vol. 13, no. 4, pp. 207–215.

Wilson, M. & Nash, J. 2003, Building an Information Technology Security Awareness and Training Program, NIST Special Publication 800-50 edn, National Institute of Standards and Technology, USA

References not used in text

"Security Awareness Tools", 98, Information Security Journal: A Global Perspective, vol. 6, no. 4, pp. 6-7.

Banking on Confidence 2010, , ISMG Information Security Media Group, U.S.A.

Glossary of Terms 2009, 13/07-last update [Homepage of Human Resources and Skills Development Canada], [Online]. Available: http://www.hrsdc.gc.ca/eng/workplaceskills/oles/2009/glossary.shtml [2010, 11/11].

Agarwal, R., Rastogi, S. & Mehrotra, A. 2009, "Customers' perspectives regarding e-banking in an emerging economy", Journal of Retailing and Consumer Services, vol. 16, no. 5, pp. 340-351.

Aladwani, A.M. 2001, "Online banking: a field study of drivers, development challenges, and expectations", International Journal of Information Management, vol. 21, no. 3, pp. 213-225.

Allen, R.K. 2004, "Legal Implications of Security Awareness in Design and Construction Practice", Journal of Professional Issues in Engineering Education & Practice, vol. 130, no. 3, pp. 208-209.

Au, Y.A. & Kauffman, R.J. 2008, "The economies of mobile payments: Understanding stakeholder issues for an emerging financial technology application", Electronic Commerce Research and Applications, vol. 7, no. 2, pp. 141-164.

Beautement, A. & Sasse, A. 2009, "The economics of user effort in information security.", Computer Fraud & Security, vol. 2009, no. 10, pp. 8-12.

BSI 2005, Information Technology - Security Techniques - Code of Practice for Information Security Management, BSI, UK.

Carnevale, D. 2003, "Awareness of Computer-Security Threats is still Inadequate, Report Warns", Chronicle of Higher Education, vol. 50, no. 12, pp. 30-30.

Chipperfield, C. & Furnell, S.M. 2010, "From security policy to practice: Sending the right messages", Computer Fraud & Security, vol. 2010, no. 3, pp. 13-19.

Courtney Jr., R. & Lipner, S. 1995, An Introduction to Computer Security: The NIST Handbook, NIST, U.S.A.

de Leeuw, K. & Bergstra, J. (eds) 2007, History of computer crime, First edn, Elsevier B.V., U.S.A.

Desman, M.B. 2003, "The Ten Commandments of Information Security Awareness Training", Information Systems Security, vol. 11, no. 6, pp. 39-44.

Etsebeth, V. & von Solms, B. 2004, Legal Implications of Information Security Governance., Masters edn, University of Johannesburg, Johannesburg.

Furnell, S.M. 2007, "Phishing: can we spot the signs?", Computer Fraud & Security, vol. 2007, no. 3, pp. 10-15.

Furnell, S.M. & Karweni, T. 1999, "Security implications of electronic commerce: a survey of consumers and businesses", Internet Research: Electronic Networking Applications and Policy, vol. 9, no. 5, pp. 372-382.

Furnell, S.M. & Network Research Group 2006, "Securing the home worker", Network Security, vol. 2006, no. 11, pp. 6-12.

Furnell, S.M., Tsaganidi, V. & Phippen, A. 2008, "Security beliefs and barriers for novice Internet users", Computers & Security, vol. 27, no. 7 - 8, pp. 235-240.

Gaunt, N. 2000, "Practical approaches to creating a security culture", International Journal of Medical Informatics, vol. 60, no. 2, pp. 151-157.

Golnaz, E., Yu, E. & Zannone, N. 2010, "A vulnerability-centric requirements engineering framework: analyzing security attacks, countermeasures, and requirements based on vulnerabilities", Requirements Engineering, vol. 15, no. 1, pp. 41-62.

Goucher, W. 2009, "The challenge of security awareness training", Computer Fraud & Security, vol. 2009, no. 10, pp. 15-16.

Goucher, W. 2008, "Getting the most from training sessions: the art of raising security awareness without curing insomnia", Computer Fraud & Security, vol. 2008, no. 4, pp. 15-15.

Granova, A. & Eloff, J.H.P. 2004, "Online banking and identity theft: who carries the risk?", Computer Fraud & Security, vol. 2004, no. 11, pp. 7-11.

Helander, M.G. & Khalid, H.M. 2000, "Modeling the customer in electronic commerce", Applied Ergonomics, vol. 31, no. 6, pp. 609-619.

Hensmans, M., van den Bosch, F.A.J. & Henk, W. 2001, "Clicks vs. Bricks in the Emerging Online Financial Services Industry", Long Range Planning, vol. 34, no. 2, pp. 231-247.

Hinde, S. 2002, "Security surveys spring crop", Computers & Security, vol. 21, no. 4, pp. 310-321.

Hoo, K.J.S. 2000, "How much is enough? A risk management approach to computer security", Workshop on Economics and Information Security, UC Berkeley, CACiteseer, .

Johnson, E.C. 2006, "Security Awareness: switch to a better programme", Network Security, vol. 2006, no. 2, pp. 15-18.

Kritzinger, E. & Smith, E. 2008, "Information security management: An information security retrieval and awareness model for industry", Computers & Security, vol. 27, no. 5 - 6, pp. 224-231.

Liao, Z. & Cheung, M.T. 2002, "Internet-based e-banking and consumer attitudes: an empirical study", Information & Management, vol. 39, no. 4, pp. 283-295.

Littler, D. & Melanthiou, D. 2006, "Consumer perceptions of risk and uncertainty and the implications for behaviour towards innovative retail services: The case of Internet Banking", Journal of Retailing and Consumer Services, vol. 13, no. 6, pp. 431-443.

McCarthy, B. 2006, "Close the Security Disconnect Between Awareness and Practice", Electronic Design, vol. 54, no. 19, pp. 20-20.

Murray, B. 2003, Generally Accepted Information Security Principles (GAISP) Version 3.0, Information Systems Security Association, U.S.A.

Osborne, M. 2006, "Information Security Laws and Regulations" in How to Cheat at Managing Information Security, pp. 71-86.

Palmer, M.E. 2001, "Information Security Policy Framework: Best Practices for Security Policy in the E-Commerce Age", Information Systems Security, vol. 10, no. 2, pp. 13-27.

Price, K. 2010, The Top 10 Information Security Threats of 2010, Inside Tech, U.S.A. (insidetech.monster.com).

Rees, J., Bandyopadhyay, S. & Spafford, E.H. 2003, "PFIRES: A Policy Framework for Information Security", Communications of the ACM, vol. 46, no. 7, pp. 101-106.

Russell, D. & Gangemi, G. 1991, Computer security basics, O'Reilly Media.

Schultz, E. 2004, "Security training and awareness - fitting a square peg in a round hole", Computers & Security, vol. 23, no. 1, pp. 1-2.

Sheehan, K.B. & Hoy, M.G. 2000, "Dimensions of privacy concern among online consumers", Journal of Public Policy & Marketing, vol. 19, no. 1, pp. 62-73.

Shwaig, K.S., Kane, G.C. & Storey, V.C. 2006, "Compliance to the fair information practices: How are the Fortune 500 handling online privacy disclosures?", Information & Management, vol. 43, no. 7, pp. 805-820.

Spurling, P. 1995, "Promoting security awareness and commitment", Information management and computer security, vol. 3, pp. 20-20.

Trombly, M. 2000, "Bankers Group Pushes Its Seal of Approval.", Computerworld, vol. 34, no. 33, pp. 20-20.

Tsohou, A., Kokolakis, S., Karyda, M. & Kiountouzis, E. 2008, "Investigating Information Security Awareness: Research and Practice Gaps", Information Security Journal: A Global Perspective, vol. 17, no. 5/6, pp. 207-227.

van Niekerk, J.F. & von Solms, R. 2009, "Information security culture: A management perspective", Computers & Security, vol. In Press, no. Corrected Proof.

Verton, D. 2000, "Companies Aim to Build Security Awareness", Computerworld, vol. 34, no. 48, pp. 24-24.

von Solms, B. 2006, "Information Security - The Fourth Wave", Computers & Security, vol. 25, no. 3, pp. 165-168.

von Solms, B. 2000, "Information security-The third wave", Computers & Security, vol. 19, no. 7, pp. 615-620.

von Solms, S.H. & Geldenhuys, J.H.S. 2001, "Information Security - A Multidimensional Discipline", Computers & Security, vol. 20, no. 6, pp. 504-508.

Whitman, M.E. & Mattord, H.J. 2007, Principles of information security, Course Technology Ptr.

Yiu, C.S., Grant, K. & Edgar, D. 2007, "Factors affecting the adoption of Internet Banking in Hong Kong - Implications for the banking sector", International Journal of Information Management, vol. 27, no. 5, pp. 336-351.

Zeichner, L.M. 2001, "Developing an overarching legal framework for critical service delivery in America's cities: Three recommendations for enhancing security and reliability", Government Information Quarterly, vol. 18, no. 4, pp. 279-291.

Article submitted to ISSA 2011

A Comparison of Best Practice Recommendations and Legal Requirements for South African banks when raising Information Security Awareness amongst Home Users of Online Banking

Carla-Lee Botha, Dr Elmarie Kritzinger[1], Marianne Loock[2]
School of Computing, University of South Africa, Pretoria
1. kritze@unisa.ac.za; 2. loockm@unisa.ac.za

Abstract— South African home users of the Internet use the Internet to perform various everyday functions. These functions include, but are not limited to, online shopping, online gaming, social networking and online banking. Home users of online banking face multiple threats, such as phishing and social engineering. These threats come from hackers attempting to obtain confidential information, such as online banking authentication credentials, from home users. It is, thus, essential that home users of online banking be made aware of these threats, how to identify them and what countermeasures to implement to protect themselves from hackers. In this respect, information security awareness (ISA) programmes are an effective way of making the home users of online banking aware of both the threats they face and the countermeasures available to protect themselves from these threats.

There are certain legal requirements with which South African banks have to comply when implementing ISA initiatives. Non-compliance or failure to demonstrate due care and due diligence should a security incident occur will result in financial penalties for the bank as well as possible brand damage and loss of customers. Banks implement international best practice recommendations in an effort to comply with legislation. These include recommendations for information security awareness.

This research investigated both information security best practice recommendations and information security legal requirements for information security awareness. A selected list of information security best practices was investigated for best practice recommendations while a selected list of information security legislation was also investigated for legal requirements imposed on South African banks. A gap analysis was performed on both these recommendations and requirements to determine whether the implementation of best practice recommendations results in compliance with legal requirements. The gap analysis found that the implementation of best practice recommendations does not result in compliance with legal requirements. Accordingly, the outcome of this research highlighted the importance of understanding the legal requirements and ensuring that adequate controls are in place with which to achieve compliance.

Keywords: information security awareness, online banking, home users, legislation, best practice, South Africa

I. INTRODUCTION

South Africans use the Internet for business purposes and at home. Home users, who have access to the Internet, use the Internet to perform various functions on a daily basis. These functions include online shopping, online gaming, social networking and online banking. Online banking is a system which allows home users to conduct their banking over the Internet (Investorwords, 2011). Online banking is a convenient way in which to carry out banking tasks, such as managing bank accounts, checking an account transaction history, transferring money and paying accounts. Online banking eliminates the need to travel to a bank each time the customer has to complete a transaction, giving individuals the option to bank in the comfort of their own homes.

It has become evident in the South African media as major banks launch advertising campaigns displaying the benefits of this service and encouraging home users to make use of this convenient form of banking. The number of internet users in South Africa has increased from 2.4 million users in 2000 to 5.3 million users in 2009

(South Africa Internet Usage and Marketing Report, 2009). Therefore, a large number of South African home users are becoming aware of and are able to use online banking. From a security perspective, the human element of the security chain must be addressed (Albrechtsen, 2007; Da Veiga & Eloff, 2010; Siponen, 2001).

While convenient, home users face multiple threats when online banking, such as phishing and social engineering. These threats emanate from hackers attempting to obtain confidential information from home users, for example, online banking authentication credentials. It is, thus, essential that the home users of online banking be made aware of these threats, how to identify them and the countermeasures available to protect themselves from the hackers' attempts.

An information security awareness (ISA) programme is an effective means of doing this. Information security awareness (ISA) comprises one component of an information security programme and it is associated with the education of the end users of an information technology system on relevant information security threats and countermeasures (Wilson & Nash, 2003). This research addresses the responsibilities incumbent on South African banks for the information security awareness of South African home users of online banking.

This research will investigate both information security best practice recommendations and information security legal requirements for information security awareness. A selected list of information security best practices will be investigated for best practice recommendations while a selected list of information security legislation will also be investigated for legal requirements imposed on South African banks. A gap analysis will be performed on both these recommendations and requirements to determine whether implementation of ISA best practice recommendations results in compliance with ISA legal requirements.

II. CURRENT AND PREVALENT THREATS TO ONLINE BANKERS

Online banking has multiple information security threats associated with its use. This research investigates the latest and most prevalent information security threats facing the home users of online banking. These threats create the need for legislation to regulate information security in the banking industry and motivate for the implementation of information security initiatives like an ISA programme. The objective of the analysis is to create a "Top 10" list of threats facing home users of online banking. These threats are matched with countermeasures that the home user may implement. Selected electronic sources are analysed for information on information security threats. Accordingly, the sources used to identify these threats should have the following attributes:

- an information security focus
- published content, written in the last two years, on current security topics
- include, in their reporting, security threats which would target the home users of online banking

The electronic sources selected are:

- SANS (www.sans.org);

- National Cyber Security Alliance (www.staysafeonline.org);
- CSOOnline (www.csoonline.com);
- CIO (www.cio.com);
- Bankinfosecurity (www.bankinfosecurity.com); and,
- Elsevier academic papers (accessed online via UNISA Library).

Although this is not an exhaustive list, for the scope of this research these sources may be considered sufficient. Each of these electronic sources have been analysed for information security threats facing the home users of online banking. The results have been narrowed down, based on frequency, to a top 10 list of information security threats facing home users of online banking. These threats are:

- phishing
- spoofed websites
- keystroke logging
- malware
- social Engineering
- minimal protection to data
- password guessing or theft
- sensitive information in the user's recycle bin
- shared computer threats
- out of date patches and software

The most prevalent information security threats facing the home users of online banking extracted from the identified electronic sources are those aiding identity theft.

III. INFORMATION SECURITY AWARENESS BEST PRACTICE

In industry, organisations attempt to gain a competitive edge by providing a better service or product. Methods and procedures used to provide services or produce products are reviewed and improved over time to try to achieve an optimal way of doing things. The methods and procedures considered at the time to produce the most desirable outcome become known as industry best practice. A best practice is a procedure or method which is known to achieve the best possible results (BusinessDictionary, 2011; Methods & tools QA Resources, 2009; Wikipedia, 2010). In this section, focus is placed on information security best practices and international standards. Information security best practices and international standards are important for effective information security governance (von Solms and von Solms, 2004). Banking organisations implement best practices for a number of reasons. These include improving customer confidence in the banks' security programmes and ensuring their information security programmes are at a standard where, should a security breach occur, they are able to demonstrate due care and due diligence and avoid financial and legal consequences (von Solms and von Solms, 2004; Williams, 2008).

This research investigates what recommendations internationally recognised information security best practices offer organisations regarding user awareness. The criteria for the selection of the best practices to be included in this research include the following:

- it must be an internationally accepted information or information security standard which can be implemented in a banking organisation
- it must be available to the public

Based on these criteria, ISO/IEC 27001, COBIT (Version 4.1) and the Standard of Good Practice for Information Security (2007) have been selected and are analysed for information security awareness recommendations. This is not an exhaustive list, but for the scope of this study, these sources are sufficient. The objective of the analysis is to create a list of recommendations organisations must implement when striving to comply with international information security best practices. The recommendations extracted from the selected information security best practices are:

A. Banks should identify what the home users of online banking need to be made aware of through the medium of ISA programmes, for example, threats and countermeasures.
B. Banks should identify the home users of online banking as a target audience for user awareness programmes and ensure that awareness materials reach all the home users of online banking.
C. Banks should conduct surveys on the level of security awareness amongst the home users of online banking after the implementation of an ISA programme. These results should serve as an input for improving the next ISA programme.
D. Banks should make home users aware of incident-reporting procedures and expected response times.
E. Banks should conduct a survey amongst home users on their level of satisfaction with the response to online banking incidents reported. These results should be used to improve the incident response procedure. Home users of online banking should then be made aware of new incident reporting procedures and incident response times.
F. Banks should make the home users of online banking aware of ways in which they may protect their information.
G. Banks should make home users aware of, and require them to comply with, certain security requirements as stipulated in the information security policy before signing up for online banking.
H. Banks should demonstrate to the home users of online banking that the banks adopt an uncompromising position in respect of information security management and awareness.

In summary, banks should identify what home users should be made aware of through an ISA programme, provide a facility for home users to report incidents and review incidents and feedback from home users to determine how ISA programmes can be improved.

IV. INFORMATION SECURITY AWARENESS LEGISLATION

Online banking is convenient, but has many information security threats associated with its use. The presence of these information security threats and their consequences motivates for regulation in the industry, increasingly making information security the subject of national and global legislation (Gerber & von Solms, 2008). This research investigates what requirements selected legislation

imposes on South African banks for information security awareness amongst the home users of online banking.

Legislation was selected based on an interview with Mra Khwar Nyo. Mra is an attorney and Certified Information Privacy Professional (International Association of Privacy Professionals) working in the Security and Privacy Services team at Deloitte & Touche, South Africa. Mra was consulted for her opinion on which legislation should be included in this study. She advised on international banking legislation, South African legislation and suggested other relevant documents. A visit to the South African government's website for publicly available documents was carried out to research other pertinent documents and identify relevant amendments to the final list of documents. The identified legislation is:

- Basel II;
- Sarbanes-Oxley Act of 2002;
- Gramm-Leach-Bliley Act of 1999;
- Electronic Communications and Transactions Act, 2002 ;
- Protection of Personal Information Bill;
- Promotion of Access to Information Act, 2000;
- The Code of Banking Practice;
- Consumer Protection Act, 2008; and,
- Constitution of the Republic of South Africa;
- Code of Governance Principles for South Africa (King III), 25 February, 2009; and,
- Electronic Communications Act, 2005.

This is not an exhaustive list, but for the scope of this study, these sources are sufficient. The objective of the analysis is to create a list of legislative requirements South African banks must satisfy when implementing an ISA programme aimed at the home users of online banking. The legal requirements extracted from the selected legislation are:

1. Banks should identify the home users of online banking as a target audience for user awareness programmes and ensure awareness materials reach all the home users of online banking.
2. Banks should make consumers aware, in plain language, of any risk associated with the online banking service that an ordinarily alert consumer would not expect.
3. Banks should promote a culture of cybersecurity by developing and implementing an ISA programme aimed at home users of online banking.
4. Banks should make home users of online banking aware that they take a stern stance on the security of online banking transactions and privacy of personal information.
5. The bank should make timely and frequent public disclosures of information which will assist the public to determine how effective a bank is at risk identification, assessment, monitoring and control. This should include the use of an independent auditor.
6. Banks should make home users of online banking aware of the threats they face when online banking, including threats to the privacy of their personal

information, and recommend countermeasures they should implement to mitigate the associated risks.

7. Banks should make antivirus software available to home users of online banking.
8. Banks should make home users aware of incident reporting procedures and expected response times.
9. Banks should review the content of ISA programmes to include new threats, changes in incident reporting procedures and response times and make home users aware of these new threats.
10. Banks should make the home users of online banking aware of their privacy policy, dealing with disclosure and protection of customers' non-public personal information. This should be done upon initiation of the customer relationship and annually thereafter until the relationship is terminated.
11. Banks should make home users of online banking aware that their personal information will only be collected and processed for legitimate purposes and retained only for as long as required by these purposes. The purposes for collection and processing should be explained to the home user before collection or processing takes place.
12. Banks should make the home users of online banking aware that they will be notified if it can be established that their personal information has been compromised.
13. Banks should make home users aware that they are entitled to confirm what personal information is held for the purpose of online banking as well as update or delete, or request to be updated or deleted, personal information held by the bank for the purpose of online banking.
14. Banks should make home users of online banking aware that they will be informed should a requestor other than the home user attempt to access their personal information or financial information. The bank should also inform the home user of their rights to refuse access to their personal information by the requestor.
15. Banks should recommend to personal clients using online banking that they review their bank statements and reconcile their accounts on a regular basis.
16. Banks should make personal clients using online banking aware that security of their personal computer is the responsibility of the personal client.
17. Banks should recommend to personal clients using online banking that they read and understand the terms and conditions associated with the online banking service before signing up for the service.
18. Banks should recommend to personal clients using online banking that they be careful to enter accurate transaction information as transactions cannot be reversed without the recipient's consent.

In summary, banks need to demonstrate to home users a stern stance on information security, make home users of online banking aware of the risks they face when making use of the online banking service and advise home users on what personal information they need to keep confidential.

V. COMPARISON OF BEST PRACTICE RECOMMENDATIONS AND LEGAL REQUIREMENTS

There is a close link between information security best practice and legislative requirements for information security, making them hard to separate (British

Standards Institution, 2005; King Committee on Governance, 2009). For example, in control section A.15, international best practice ISO/IEC27001 deals with compliance with legislative requirements, including laws, regulations, statutes and contractual obligations. Also, compliance with legislative requirements can be achieved by implementing best practice controls, such as implementing COBIT to comply with Sarbanes-Oxley. Compliance ensures that, should a legislative breach occur, the organisation is able to demonstrate due care and due diligence, avoiding financial and legislative consequences (von Solms & von Solms, 2004; Williams, 2008).

In section 3 and section 4, ISA best practice recommendations and ISA legal requirements were identified. In this section, a comparison between these recommendations and requirements is made to determine if implementation of the identified ISA best practice recommendations will result in compliance with the identified ISA legal requirements. Figure 1 illustrates the gap between the selected legal requirements and selected best practice recommendations by showing which best practice requirements support each legal requirement.

Finding 1: The results show that the implementation of the selected best practice recommendations would fully satisfy seven of the 18 legal requirements only and partially satisfy the other nine. There are no other recommendations offered for two of the 18 legal requirements.

Finding 2: Compliance with legal requirements 1 to 4, 6, 8 and 17 may be achieved through the implementation of best practice recommendations.

Finding 3: Legal requirement number 5 is partially satisfied by the selected best practices. Selected best practices require a bank to demonstrate a stern stance on risk management, but do not explicitly require a bank to disclose incidents which would be material to the home users' decisions to continue making use of the online banking service.

Finding 4: Legal requirements number 7 is partially satisfied by the implementation of best practice recommendations. The selected best practice recommendations do not explicitly require banks to make security software available to home users of online banking, as required by legal requirement number 7. However, the selected best practices recommend that banks make home users of online banking aware of countermeasures they can implement and recommend awareness materials reach all home users. Security software may be included in the awareness materials;

Finding 5: Legal requirement number 9 is only partially satisfied by the implementation of selected best practice recommendations. The recommendations do not state the need to update the content of the ISA programme to include new threats. However, the Standard of Good Practice for Information Security statement UE6.2.6 recommends that banks should review security incidents and use findings to update the next ISA programme aimed at home users of online banking. Such a review would reveal previously unidentified threats to home users of online banking.

Finding 6: Although the selected best practices recommend that banks make home users aware of how they can protect their personal information, legal requirements 10 to 15 suggest that best practices do not offer sufficient

guidance on ensuring privacy of personal information. However, the Standard of Good Practice for Information Security section UE6.1 does address information privacy, recommending that banks develop and implement approved methods for handling personally identifiable information.

Finding 7: No matches for legal requirements numbers 16 and 18 suggest that the selected best practices do not stipulate the need for home users to be made aware of what their responsibilities are when protecting themselves.

It may, thus, be concluded that implementing the ISA recommendations identified in the selected best practices does not result in compliance with the ISA requirements identified in the selected legislation.

VI. CONCLUSION

A large number of South African home users are becoming aware of and are able to use online banking, facing multiple information security threats while they do so. From a security perspective, the human element of the security chain must be addressed. Therefore, the focus of this research has been on home users and the actions South African banks are required and recommended to take when implementing Information Security Awareness (ISA) programmes aimed at home users of online banking.

South African banks need to protect their home users from the information security threats they face as online bankers, be able to demonstrate due care and due diligence when addressing these information security threats by implementing best practice, and they must recognise and comply with the legal requirements imposed on them.

This research set out to determine if implementation of selected best practice recommendations for information security awareness will result in compliance with ISA legal requirements placed on South African banks when raising information security awareness amongst the home users of online banking. Findings demonstrate that implementation of the identified best practice recommendations does not result in compliance with the identified legal requirements.

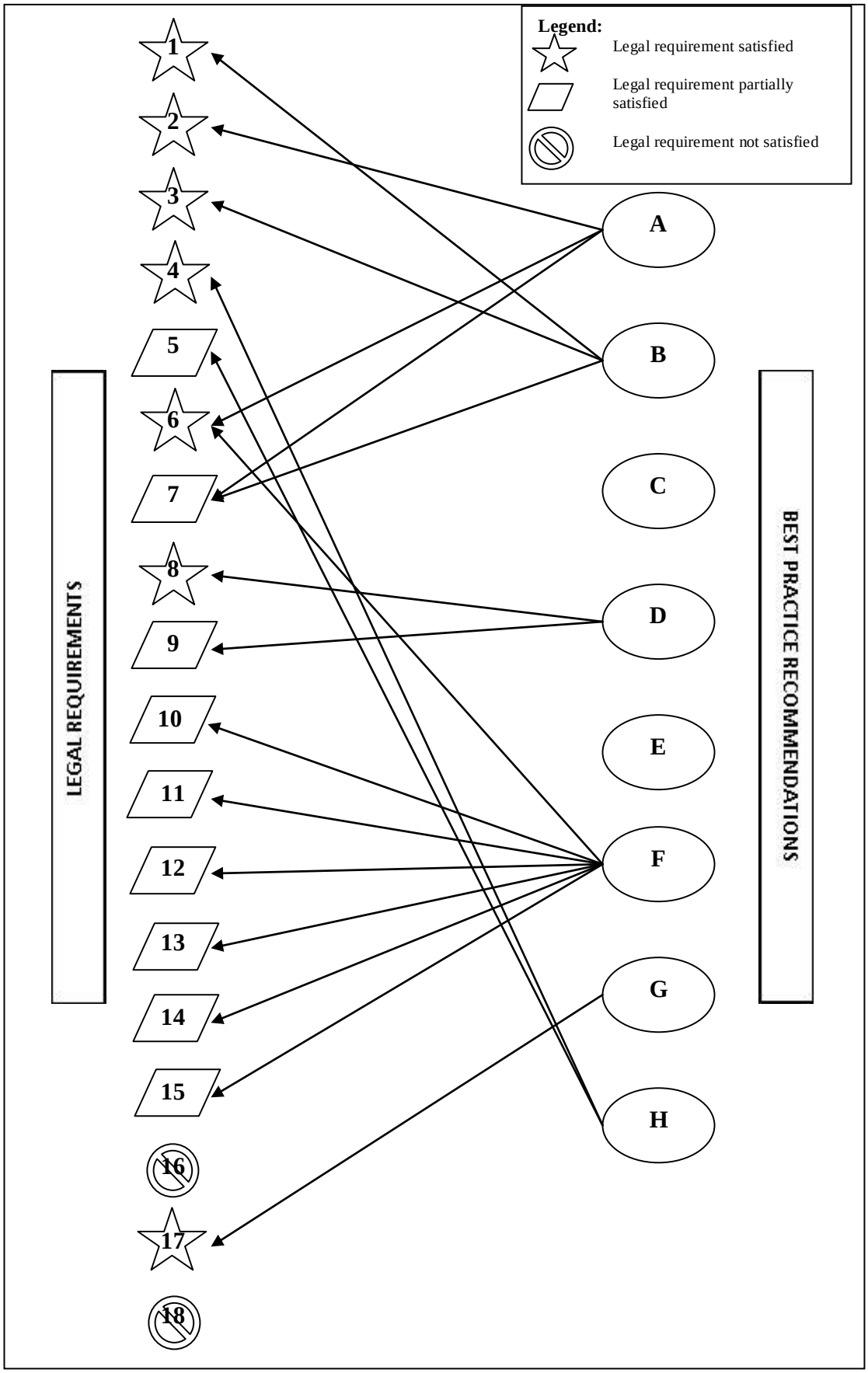


Figure 1 Comparison of legal requirements and best practice recommendations

References

Albrechtsen, E. 2007, "A qualitative study of users' views on information security", *Computers & Security,* vol. 26, no. 4, pp. 276–289.

British Standards Institution 2005, *BS ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements*, 2005th edn, British Standards Publishing Limited.

BusinessDictionary 2011, 2011–last update, *BusinessDictionary* [Homepage of WebFinance, Inc], [Online]. Available: http://www.businessdictionary.com/definition/best-practice.html [2011, 03/31].

Da Veiga, A. & Eloff, J.H.P. 2010, "A framework and assessment instrument for information security culture", *Computers & Security,* vol. 29, no. 2, pp. 196–207.

Gerber, M. & von Solms, R. 2008, "Information security requirements: interpreting the legal aspects", *Computers & Security,* vol. 27, no. 5–6, pp. 124–135.

Investorwords 2011, 2011-last update, *Investorwords* [Homepage of WebFinance, Inc], [Online]. Available: http://www.investorwords.com/3420/online_banking.html [2010, 07/06].

King Committee on Governance 2009, *Code of Governance Principles for South Africa (King III),* Institute of Directors in Southern Africa, South Africa.

Methods & Tools QA Resources 2009, 2009–last update [Homepage of Quality Assurance Project], [Online]. Available: http://www.qaproject.org/methods/resglossary.html [2010, 11/11].

Siponen, M.T. 2001, "Five dimensions of information security awareness", *ACM SIGCAS computers and society,* vol. 31, no. 2, pp. 24-29.

*South Africa Internet Usage and Marketing Report*2009, 2009–last update [Homepage of Miniwatts Marketing Group], [Online]. Available: http://www.internetworldstats.com/af/za.htm [2010, 07/06].

von Solms, B. & von Solms, R. 2004, "The 10 deadly sins of information security management", *Computers & Security,* vol. 23, no. 5, pp. 371–376.

Wikipedia 2011, 17/02/2011–last update, *Wikipedia* [Homepage of Wikimedia Foundation, Inc], [Online]. Available: http://en.wikipedia.org/wiki/Best_practice [2010, 11/11].

Williams, P.A.H. 2008, "In a 'trusting' environment, everyone is responsible for information security", *Information Security Technical Report,* vol. 13, no. 4, pp. 207–215.

Wilson, M. & Nash, J. 2003, *Building an Information Technology Security Awareness and Training Program*, NIST Special Publication 800-50 edn, National Institute of Standards and Technology, USA.