University of Cape Town

Department of Information Systems

Understanding the effects of user participation in Information Security Risk Management: A comparative study of South Africa and Malawi

A thesis submitted in partial fulfilment of the requirements for the degree of

Master of Commerce in Information Systems

By

Dimson Kalelo-Phiri

Supervised by Professor Michael Kyobe

September, 2012

Plagiarism Declaration

1. I know that plagiarism is wrong. Plagiarism is using another's work and to pretend that it is one's own.
2. I have used the American Psychological Association (APA) as the convention for citation and referencing. Each significant contribution to, and quotation in, this report from the work, or works of other people has been attributed and has been cited and referenced.
3. This report is my own work.

I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as his or her own work.

I acknowledge that copying someone else's assignment or essay, or part of it, is wrong, and declare that this is my own work

Signed by candidate

SIGNATURE: Signature Removed DATE: 28th November, 2012 .

Full name(s) of student: Dimson Kalelo-Phiri

Abstract

The concept of user participation and how this contributes to the system success has been a research interest for many researchers since 1960s. The importance of user participation in the management of information security is widely endorsed in literature. Nonetheless, users are also viewed as weak links to information security. Shared beliefs and values otherwise known as culture influence user behaviour towards information security.

Culture guides user attitude and behaviour towards information security management practices and transcends organisational boundaries. In order for the practitioners and academic community to understand how culture influences user behaviour, there is need for cross-cultural or cross-national studies. Cross-cultural studies in Information Systems (IS) have mainly focused on the relationships between culture and Information Technology (IT) development, adoption and diffusion, management, and use. Very few of cross-cultural studies have looked at cultural influence on user participation in relation to information security management.

The purpose of this study was to understand how user participation in Information Security Risk Management (ISRM) practices contributes to the efficient management of information security. The study also aimed at understanding how different cultures influence user participation in ISRM. To achieve these objectives, the study employed a mixed methods research approach to comparatively collect, analyse, and interpret data from South Africa and Malawi. Questionnaires were sent to information security administrators and information systems auditors while semi-structured interviews were conducted with users at Blantyre Water Board (BWB) in Malawi.

The findings of this study showed that user participation in ISRM practices contributes to the efficient management of information security. The findings also revealed that cultural differences are critical determinants of user participation in ISRM practices between South Africa and Malawi. Users in Malawi were found to participate more in information security awareness campaigns while users in South Africa participate more in remediating defective information security controls. In addition, governmental organisations and financial institutions are more interested in managing information security in South Africa and Malawi respectively.

The implications of these findings to practitioners as well as the academic community are discussed and areas requiring further research suggested.

Acknowledgement

Firstly, I would like to thank God, Almighty for blessing me with abundant life which enabled me to undertake my studies at University of Cape Town (UCT) throughout the whole academic period. I am thankful to God because during the entire period I never met any insurmountable challenge that would have affected my studies. His enabling hand was on me always.

Secondly, I would like to extend my sincere thanks to my supervisor Prof. Michael Kyobe for his continuous guidance and technical input which enabled me to produce this report. His effort is deeply appreciated. I would also like to thank Mr. Frank Makoza and Mr. John Mtingwi for their technical direction in the conceptualisation and execution of this study. Lastly, I am very grateful to my family members Mr. M.B. Kalelo, Hon J. Kalelo-Phiri, Mr. V.K Phiri and to my friends Mr. R. Chizimba, Dr. Mathews Kagoli and Mr. Francis Kavala for their moral support received during my studies. Their words of encouragement inspired me to work on until at the end of my studies.

Dedication

I dedicate this dissertation to my late mother Lydia and my children Brian, Tendai and Tadala.

Acronyms and abbreviations

ACCA	Association of Chartered Certified Accountants
BWB	Blantyre Water Board
CIA	Certified Internal Auditor
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CISSP	Certified Information systems Security Professional
CRISC	Certified in Risk and Information Systems Control
ECT Act	Electronic Communications and Transactions Act
ICT	Information and Communication Technologies
IS	Information Systems
ISAC	Information Security Awareness Campaigns
ISACA	Information Systems Audit and Control Association
ISCD	Information Security Control Development
ISCP	Information Security Control Performance
ISD	Information Systems Development
ISRM	Information Security Risk Management
IT	Information Technology
LDCs	Least Developed Countries
NIST	National Institute of Standards and Technology
PCI-DSS	Payment Card Industry - Data Security Standard
PREM	Poverty Reduction and Economic Management
QSA	Qualified Security Assessor
SOX	Sarbanes-Oxley
TAM	Technology Acceptance Model
TPB	Theory of Planned Behaviour
TPEU	Theory of Perceived Ease of Use
UCT	University of Cape Town

Table of Contents

List of Figures

List of Tables

Chapter 1 : Introduction

1.1 Background

Insiders such as employees, contractors, consultants, and vendors are weak links to organisation's information security (Dojkovski, Lichtenstein, & Warren, 2011; Lim, Chang, Maynard, & Ahmad, 2009; Spears & Barki, 2010; Steele & Wargo, 2007; Thomson, von Solms, & Louw, 2006). Studies have shown that insiders contribute to over 50% of the breaches to information security (Gordon, Loeb, Lucyshyn, & Richardson, 2005). In a recent study by D'Arcy, Hovav and Galletta (2009), it was found that about 50% to 70% of information security incidents originated from within organisations. This is attributed to user unauthorised access to systems (Gordon et al., 2005), user noncompliance with information security policies and procedures (Lim et al., 2009; Pahnila, Siponen, & Mahmood, 2007; Siponen & Oinas-Kukkonen, 2007). This may also come from disgruntled employees (Standage, 2002).

Contrary to the weak-link image of users to information security, users can significantly help in addressing some of the information security threats (Chang & Ho, 2006; Siponen, 2005; Spears & Barki, 2010; Stanton & Stam, 2006; Whitman, 2008). User behaviour such as being careful in handling organisation's data positively contributes to the management of information security (Stanton & Stam, 2006). In addition, Information Technology (IT) competence levels of business managers positively influence the implementation of ISRM standards as stipulated in ISO17799 and BS7799 for International Standards Organisation (ISO) (Chang & Ho, 2006). These standards enable organisations to manage and protect information by ensuring data confidentiality, integrity and availability (Tong, Fung, Huang & Chan, 2003).

These inconsistent views seem to suggest that the concept of user participation in ISRM and its impact on information security management remains unclear (Bachore & Zhou, 2009). Firstly, the purpose of this study was to understand how user participation in ISRM practices contributes to the management of information security. This was aimed at making a contribution towards the on-going discussion on the effect of user participation in ISRM practices on information security management.

Most studies on information security have been conducted at the organisational level and most of them have focused much on individual user level of information

security (Straub, 1990; Straub & Welke, 1998; Dhillon & Backhouse, 2001; Im & Baskerville, 2005; Sun, Srivastava, & Mock, 2006; Chen & Zahedi, 2009; Johnston & Warkentin, 2010; Liang & Xue, 2009; Myyry, Siponen, Pahnila, Vartiainen, & Vance, 2009). Studies focused on how inter-organisational or inter-country interactions influence user attitude and behaviour towards the management of information security are limited (Dinev, Goo, Hu, & Nam, 2009; Kwak, Kizzier, Zo, & Jung, 2011). In addition, studies that try to understand how culture shapes user behaviour towards ISRM practices (Lim et al., 2009) and establishing the effect of user behaviour on information security management between countries are also limited (Dinev et al., 2009; Kwak et al., 2011).

Culture which can be visible at individual, organisational, societal, and national level (Leidner & Kayworth, 2006), affects the way information security policies are formulated and implemented. It also affects the way users recognize information security risks (Schmidt, Johnston, Arnett, Chen, & Li, 2008). This shows, therefore, that culture plays a crucial role in influencing user participation in ISRM practices. However, it is clear that despite this established fact, not much attention has been put to further understand this relationship particularly by comparing countries within a particular region like Southern Africa. This study was done in order to understand how different cultures influence user participation in ISRM in the context of South Africa and Malawi.

South Africa and Malawi were chosen based on their different cultures according to Hofstede's culture indices of: power distance, uncertainty avoidance, individualism-collectivism, and masculinity-femininity (Dinev et al., 2009). While South Africa has a post-apartheid culture (Oosthuizen & Bhorat, 2004), Malawi comes from a 31-year of autocratic rule based on political repression (Forster, 1994). Comparing countries with different national cultures provides better insight as to how national cultures influence user participation in ISRM practices. This would further be related to the management of information security.

A mixed methods research approach was employed in this study. This approach was chosen for two reasons. Firstly, results acquired from qualitative methods were used to elaborate (complement) results acquired from quantitative methods. Secondly, the mixed methods research approach was employed to have results acquired in qualitative methods confirm (triangulate) those acquired from the quantitative methods (Migiro & Magangi, 2011). The overall strength of a mixed-

method approach is greater than either that of qualitative or quantitative research methods (Creswell, 2009).

1.2 Research objectives and questions

Firstly, the objective of this study was to understand how user participation in ISRM contributes to the efficient management of information security. Secondly, this study was aimed at understanding how different cultures influence user participation in ISRM which may have an impact on the overall management of information security. The following two questions guided the study: How does user participation in ISRM contribute to the efficient management of information security? How does the effect of user participation in ISRM vary across nations of different cultural origins?

1.3 Importance of the research

The study is important in two ways. Firstly, the findings of the study provide guidance to practitioners for dealing with information security issues in different cultures. Based on the findings of this study, information security managers should be focusing on instilling a user participation culture in ISRM practices which, in turn, would help address information security incidents. Secondly, the findings of this study provide guidance to the academic community for conducting studies which span countries of different national cultures.

1.4 Research limitations

There were a number of limitations to this study.

There was lack of a tangible study population. The study population comprised of information security administrators and information systems auditors for the survey questionnaire and end-users for semi-structured interviews. There was no local chapter for these professionals at the time of conducting the study in Malawi. This would have provided a list from where participants to the study would have been identified. Alternatively, snowball sampling method was used to identify study participants. Snowball sampling method is suitable for reaching out to populations that are difficult to contact.

There was also delayed and low response rate. The study was planned to be executed from February to August 2012. The low response rate experienced necessitated for more time in order to allow for more participants to respond. Due

to low response rate in Malawi, the researcher who was based in ate UCT in South Africa relied on reminders on by phone and emails.

The researcher also experienced low response rate on the part of South African respondents. In South Africa, the Information Systems Audit and Control Association (ISACA) Chapter consented to invite its 200 members to participate in the study. However, there was no contact between the study participants and the researcher. This was due to ISACA South Africa chapter's policy which does not allow passing of member details to third parties e.g. researchers. In an effort to follow-up on the study participants, the researcher sent reminders to the ISACA South Africa chapter office, a process which delayed and affected the response rate.

1.5 Thesis outline

The rest of the dissertation is organized into four chapters as follows:

Chapter 2 provides a summary of the literature which, in turn, creates a basis for this study. The chapter begins by introducing the concepts of user participation and culture. It then advances to discuss the concepts of Information Security Risk (ISR) and how user behaviours contribute to ISR. Concepts of organisation and information security culture and Information Security Risk Management are subsequently presented. This is followed by a research contextualisation and a summary of the literature review. The chapter recognises a few studies which provide empirical evidence of how national cultures influence the user attitude and behaviour towards ISRM practices. Lastly, Chapter 2 presents the conceptual model followed by a discussion of the model constructs.

Chapter 3 discusses the research design which largely encompasses four elements: the research philosophical assumptions, research methodology, the research timeline and ethical considerations. The research methodology covers a number of areas pertaining to the purpose of the study, the type of investigation employed in the study, the research method, survey participants, sampling method, survey instruments, data collection, and data analysis.

Chapter 4 contains the statistical analyses conducted on the collected data. The validity and reliability test results are presented in this chapter as well as the results for the hypotheses testing.

Chapter 5 summarises the study findings. The study conclusion, recommendations, practical usefulness, and suggestions for areas for future research are presented in this chapter.

Chapter 2 : Literature review

This chapter is a review of literature which demonstrates the ability of the researcher to show what is already available on the topic being studied and gaps worthy intervening (Hart, 1998; Levy & Ellis, 2006). The chapter summarises findings from studies that expound the concept of user participation as well as those which explain the influence of national cultures on user attitude and behaviour towards ISRM practices.

The chapter is organized into six sections. Section 2.1 introduces terms and concepts related to user participation and culture. Section 2.2 discusses the concepts of information security and information security risk. Section 2.3 defines organisational and information security cultures. The concept of ISRM is presented in Section 2.4. The context of the study outlined in Section 2.5. Lastly, Section 2.6 introduces the conceptual model.

2.1 User participation and culture

2.1.1 User participation

The Longman Dictionary of Contemporary English (1978) defines the term "user" as a person or thing that uses something. Based on this definition, this study used the term "user" to refer to a class of people in an organisation who use a computer or a network service. Users do not need to possess complete technical expertise to fully understand the system they use. Users handle enterprise information as they perform their daily duties.

The Longman Dictionary of Contemporary English (1978, p. 790) also defines the term "participation" as "the act of taking part or having a share in an activity or event. Based on these definitions, the term "user participation" was used in this study to imply users taking part or having a share in an activity or event. The event was defined as Information Systems Development (ISD) activity or an ISRM practice.

The concept of "user participation" in ISD and how it impacts system success has been a core research topic since 1960s (Swanson, 1974; Markus & Mao, 2004). While it is widely viewed that user participation in ISD has positive impact on system success (Jiang, Klein, & Hong-Gee, 2006; McGill & Klobas, 2008; McKeen & Guimaraes, 1997; Medina & Caparro, 2007; Rees, 1993; Terry & Standing, 2004), user participation in ISD sometimes negatively impacts the success of the system

being developed (Bachore & Zhou, 2009; He & King, 2008; Kim & Peterson, 2003). Studies have shown that user participation in ISD leads to group dysfunction (Kim & Peterson, 2003) particularly where a group does not work as a single entity and has no defined goal (Tessina, 2008). User participation in IS projects can also lead to increased project costs (He & King, 2008) as a result of contextual conflicts arising from development groups such as developers, business managers, and end-users. User participation in ISD can therefore contribute positively towards system success only if conflicts are resolved (Fakun & Greenough, 2004). This is supported by previous studies as it was once stated that:

"…user participation in the development process can negatively influence project performance since it could make the process more difficult, lengthy, and less effective. Such contradictory findings raise the question of when user participation is actually helpful and when it might negatively impact project performance" (Subramanyam, Weisstein & Krishnan, 2010, p. 137)

This shows that user participation in ISD does not always contribute to the success of the system being developed. The extract also shows the two different views portrayed in literature about the unpredictable contribution of user participation in ISD towards system success.

In the context of ISRM, users are portrayed as weak links to information security and part of the solution to addressing information security problems (Dojkovski et al., 2011; Lim et al., 2009; Spears & Barki, 2010; Steele & Wargo, 2007; Thomson et al., 2006; Chang & Ho, 2006; Siponen, 2005; Spears & Barki, 2010; Stanton & Stam, 2006; Whitman, 2008). These different views about user participation in both ISD and ISRM show that the concept of user participation is still unclear and requires more research (Bachore & Zou, 2009).

2.1.2 User culture

Culture has been defined by various authors as the manner in which a group of people solves problems and reconciles dilemmas (Trompenaars & Hampden-Turner, 1998). It has also been defined as a collective mental programming of people that distinguishes them from others (Hofstede, 2001), or the fabric meaning through which people interpret events around them (Geertz, 1973). The common theme in these definitions is that culture influences the behaviour of the people and is characterized by shared values, norms, and mutually reinforcing patterns of

behaviour amongst the members of a particular society (Steers, Meyer & Sanchez-Runde, 2008).

Guo (2008, p. 6) defines culture as "norms, beliefs, and basic assumptions shared by members of an organisation" and it includes "values, principles, norms, traditions, unwritten rules, and informal procedures" (Guo, 2008, p. 4). It promotes responsibility, integrity, trustworthiness, and ethicality of people in an organisation (Dhillon & Backhouse, 2000; Dojkovski et al., 2011). In view of culture, it may be concluded that most of the aspects of people's behaviour in organisations are culturally motivated.

Schein (1985) describes the aspects of culture at three different levels namely: basic assumptions which represent belief systems that individuals have towards human behaviour, relationship, reality and truth; values which signify espoused beliefs and identify what is important to a particular cultural group; and artefacts which may include things such as art, technology, visible behavioural patterns as well as myths (Pettigrew, 1979) which are representative of a particular culture.

According to Schein (1985), cultural values are more easily studied than basic assumptions which are invisible and artefacts which are not easily decipherable. Cultural values are seen as sets of social norms that define the rules or context for social interaction. They determine the way people act and communicate (Delong & Fahey, 2000) and have a significant impact on the behaviour of the members of an organisation. They act as means of social control and set the expectations and boundaries of appropriate behaviours for members of organisations (O'Reilly & Chatman, 1996).

Studies have shown that there are five observable characteristics of culture which relate to the behaviour of users in an organisation which include responsibility, participation, commitment, motivation, and awareness (Lim et al., 2009). These characteristics have been reflected in the conceptual model (Figure 2.4) and discussed subsequently.

Many organisations now conduct businesses beyond their organisational and national boundaries using the Information and Communications Technologies (ICTs) (Myers & Tan, 2002). According to the theory of network externalization, organisations are exposed to external threats as a result of either the users within the organisations accessing information from external sources through the internet

or customers accessing enterprise data through the internet. This exposes the organisations to information security threats which they have no control over (Anderson & Moore, 2006). It is therefore important for organisations to understand how users in different cultures behave if they are to be assured of the security of enterprise data (Ives & Javenpaa, 1991; Shore & Venkatachalam, 1996).

Organisations cannot be secure unless they become aware of how different cultures in different countries where they conduct business influence people's attitude and behaviour towards information security (Applegate, McFarlan, & McKenney, 1999; Harris & Davison, 1999). This awareness would make the organisations to put countermeasures in place which would help mitigate information security risks arising from cross-cultural business transactions.

2.2 Information security and information security risk

2.2.1 Information security

The wide use of IT, Internet, wireless networks and instant messaging make many organisations to experience losses due to the damage caused by compromises in information security (D'Arcy et al., 2009; Richardson, 2007). Information security problems cause damage to enterprise information through malware or hacker attacks, theft of proprietary information, or an insider abusing information resources (Jahner & Krcmar, 2005).

There are different viewpoints of information security which are technical, behavioural, managerial, philosophical, and organisational (Zafar & Clark, 2009). Based on these viewpoints, various authors define "information security" as the process of protecting the availability, privacy, and integrity of information (Geek, 2008). It also implies the proper use of data and controls to prevent accidental or unauthorized use, destruction, or the modification of information assets (Peltier, 2005). Information security is also a "process of protecting the confidentiality, integrity and availability of information" (Bishop, 2003, p. 67). It is a "well informed sense of assurance that information risks and controls" (Anderson, 2003, p. 310) are in balance. What is common in these definitions is that information security is about protection of information from abuse or unauthorised access.

Von Solms (2006) traces the progression of information security and defines what he refers to as "waves" of information security progression. Von Solms (2006, p. 165) characterizes the first wave as "information security being a technical issue".

During this wave, information security is perceived as technical in nature and only left for technical experts. The second wave is characterised as information security having a strong management issue where aspects like policies and management involvement become important. Information security in third wave is characterised as having some form of standardization, where aspects like best practices, certification, information security culture and the measurement and monitoring of information security becomes important. Von Solms (2006) finally characterises the fourth wave as information security having some form of governance issue.

The fourth wave of progressive development of information security (von Solms, 2006) involves the establishment of regulatory measures such as the enactment of the Electronic, Communication and Transaction (ECT) Act of 2002 enacted by the government of South Africa (Kyobe, 2009) as well as the Telecommunications Act by the Government of Malawi in 1998. Information security policies and procedures which help to ensure secure IS environments are regularly demanded by internationally accepted best practices for information security management. Best practices are essential requirements for good IT governance hence for good corporate governance (Saint-Germain, 2005).

Taking a holistic approach to information security, as is recommended in literature, information security is defined as:

> *"…understanding the potential threats of an organisation and assessing the risks associated with those threats; educating personnel in security awareness, code of conduct, and information security best practices; establishing policies and procedures to mitigate loss should security breach occur; implementing and monitoring technologies to prevent or mitigate the loss from present or future security breach; continuous assessment of technology, policies and procedures and personnel to assure proper governance of information security issues; and incorporating information security governance as an important part of corporate governance"* (Da Veiga & Eloff, 2007; Dhillon & Torkzadeh, 2006; Zafar & Clark, 2009).

Literature consistently reports of increased concern of information security in organisations and there has been an on-going proposition that information security can efficiently be managed if the focus goes beyond the technical means of protecting information resources (Baskerville, 1993; Straub & Welke, 1998; Dhillon & Backhouse, 2000; Jahner & Krcmar, 2005; Dhillon & Torkzadeh, 2006; Chang &

Ho, 2006; Bednar & Katos, 2009). For instance, Bednar and Katos (2009) express the need for information security management to not only view the human factor as an obstacle but rather as an enabler. Realising the importance of the human factor in information security, the Editor-in-Chief of one of the respected journals, "Computers & Security", observed that the human factor in information security deserves greater research attention (Schultz, 2005).

While it is important for organisations to have sophisticated tools to deter information security from outside, it is difficult to protect against users. Users intimately know the internal operations and business processes and have access to enterprise data (Steele & Wargo, 2007). One approach advanced in previous studies is to address the information security concern in organisations is the introduction of sanctions based on the deterrence theory (Siponen & Oinas-Kukkonen, 2007). This approach assumes that fear of sanctions influences users to comply with the information security policies that are in place (Akers & Sellers, 1994; Siponen & Oinas-Kukkonen, 2007; Straub & Straub, 1990). Sanctions result in reduced computer abuse (Straub & Straub, 1990) and increase employee compliance with security policies (Siponen & Oinas-Kukkonen, 2007). According to the General Deterrence Theory (GDT), procedural and technical information security countermeasures serve as deterrent mechanisms. Deterrent mechanisms increase perceived threat of punishment for IS misuse (D'Arcy et al., 2009).

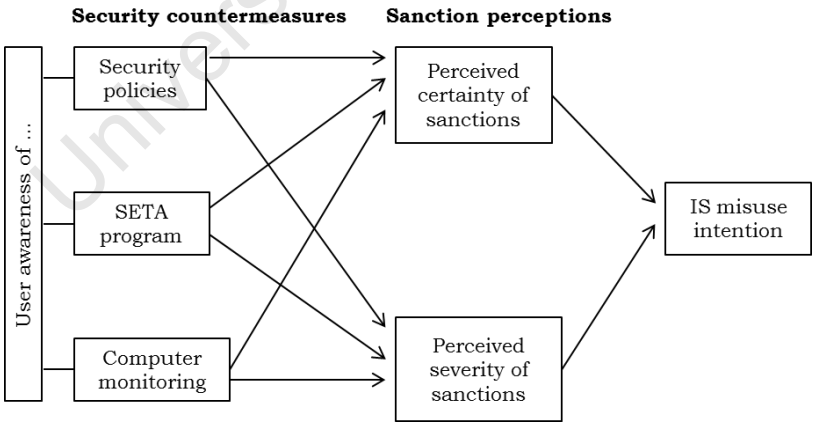

Figure 2.1: The GDT Model (D'Arcy et al., 2009)

As can be noted from the GDT model in Figure 2.1, the countermeasures include security policies, security education, training and awareness (SETA) programs, and computer monitoring. These countermeasures function like societal laws in providing knowledge of what constitutes acceptable and unacceptable conducts

thereby increasing perceived threats of punishment for offenders (Lee & Lee, 2002). The deterrent effect of SETA programs is achieved through security awareness briefings or trainings which enforce acceptable usage guidelines and further emphasize potential consequences for IS misuse (D'Arcy et al., 2009). The GDT model shows that user awareness about the security countermeasures directly impacts user perceptions of the certainty and severity of sanctions associated with IS misuse (D'Arcy et al., 2009).

Information security is broken down into policies, technology, and procedures (Adams, Templeton, & Campbell, 2007). An information security policy is a document which outlines "individual responsibilities, define authorized and unauthorized uses of the systems, provide venues for employee reporting of identified or suspected threats to the system, define penalties for violations, and provide a mechanism for its update" (Whitman, 2004, p. 52). Compliance with information security policies and legislation is noted as critical to organisations as well as educational institutions (Kyobe, 2010). Secondly, information security in form of technology is the artefact that allows users in an organisation to protect the information system. A typical example of information security technology is antivirus software. Information security procedures are methodologies or guidelines which are followed in order to protect information systems (Nyanchama, 2005). Information security management therefore ensures that these three forms of information security are in place and are up-to-date.

2.2.2 Information security risk (ISR)

There are many definitions for the word "risk" reflecting that it means different things to different people. For instance, risk is defined as the potential that a given threat will exploit vulnerabilities of an asset thereby causing some sort of damage to the organisation (Vedder, 1998). Risk is also defined as "a function of the likelihood of a given threat-source's exercising a particular potential vulnerability and the resulting impact of that adverse event on the organisation" (Stoneburner et al., 2002, p. 8). According to the economic theory of risk and insurance which was originally published by Allan Willett in 1901, risk is defined as the objectified uncertainty as to the occurrence of an undesired event. The underlying concept in these definitions is that risk is a chance or possibility that an unwarranted condition or behaviour takes advantage of existing weaknesses (vulnerability) in an asset to cause damage to the organisation. Risk is the probability that an

investment's actual return will be different from that which is expected (Stoneburner, Goguen, & Feringa, 2002).

It is practically impossible for organisations to completely escape risk. Consequently, Tsiakis and Stephanides (2005) suggest some ways in which organisations can deal with risk: accepting it, ignoring it (avoidance), assigning it to someone (risk transfer), or mitigating. Risk acceptance is an approach where an organisation decides to bear the consequences or impact that may result from an information security incident. One aspect of risk acceptance is self-insurance. An organisation may choose not to perform any activity (e.g. not installing an application) that could have a potential risk as a way of avoiding information security risks. Thirdly, risk mitigation involves taking some action aimed at reducing the impact of an information security incident. Typical examples of risk mitigation include use of effective access control mechanisms, patching of systems, and firewalls and intruder detection systems (IDSs). Another way of dealing with risk is by transferring it to another party by either contract or insurance cover. In this way, liability is transferred to either contractors or suppliers (Jones, 2007; Stoneburner et al., 2002; Tsiakis & Stephanides, 2005).

While business risks include concerns about probable effects of an uncertain event on achieving established business objectives, information security risk concerns the availability and reliability of IT services (ISACA, 2008). There are five economic impediments to information security management: information asymmetries, externalities, liability, diversity, and the fragmentation of legislation and law enforcement (Anderson & Moore, 2006). Information asymmetry refers to a situation where one organisation has better or more information than others which makes it to have more power when making decisions during transactions (Kyobe, Matengu, Walter & Shongwe, 2012). Information asymmetry becomes an impediment to information security management because organisations with more power are not usually willing to discuss their weaknesses with those organisations with poor information hence less powerful. Information asymmetry can be a major problem when organisations wish to have coordinated efforts to managing information security (Anderson & Moore, 2006).

Secondly, many information security threats are attributed to network externalities (Anderson & Moore, 2006). Enterprise networks today are connected to external environments (simply referred to as externalities) which are not always secure. It is

difficult to have protective measures in an organisation when its network has been externalized. Network externalization refers to allowing access to an enterprise network by customers from outside the organisation. It also means users within an organisation accessing information from outside sources using the internet (Anderson & Moore, 2006). Network externalization is an impediment to information security management because it exposes an organisation to external threats that the organisation has no control over.

In liability dumping, organisations that seek to manage information security risk often dump it on less powerful suppliers or customers. Sometimes, software and service suppliers impose licenses on customers and disclaim all liability as well as information security failures (Anderson & Moore, 2006). Also, lack of diversity is a concern against platform vendors. Lack of diversity makes successful attacks more devastating and hard to insure against. Fragmentation of legislation and law enforcement concerns lack of international legislation which would help to curb information security perpetrators globally. One country may have strong legislation and with the presence of the internet, offenders have numerous options to operate from other countries where there are weak or no regulatory measures against information security breaches.

Information security risk can also be explained by looking at the components that it is made up of which include assets, threats, and vulnerability (Adams et al., 2007). Security threats are circumstances that have the potential to cause loss or harm (Pfleeger, 1997). Security threats may come from within and outside the organisation (Hinde, 2002). Examples of internal threats are "mistakes by employees" (Mitchell, Marcella, & Baxter, 1999) while viruses (De Campeaux, 2002) and attacks by hackers (Austin & Darby, 2003) are the most cited types of external threats. Associated with security threats are threat-sources. Threat-sources are "either an intent and method targeted at the intentional exploitation of vulnerability or a situation and method that may accidentally trigger vulnerability" (Stoneburner et al., 2002, p. 12). Common threat-sources are natural (floods, earthquakes, tornadoes, landslides, avalanches, and electrical storms), human events that are either enabled by or caused by human beings (unintentional acts, inadvertent data entry) or deliberate actions (network based attacks, malicious software upload, unauthorized access to confidential information), or environmental (long-term power failure, pollution, chemicals, liquid leakage). Security vulnerability is a "weakness that can be accidentally triggered or intentionally exploited by a threat-

source (Stoneburner et al., 2002). Table 2.1 outlines various threat-sources, their motivation and threat actions according to Stoneburner et al (2002).

Threat sources	Motivations	Threat actions
Hacker, cracker	• Challenge • Ego and rebellion	• Hacking • Social engineering • System intrusion • Unauthorised system access
Computer criminal	• Destruction of information • Illegal information disclosure • Monetary gain • Unauthorized data alteration	• Computer crime (e.g. cyber stalking) • Fraudulent act (e.g. replay, impersonation, interception) • Information bribery • Spoofing • System intrusion
Terrorist	• Blackmail • Destruction • Exploitation • Revenge	• Bomb/terrorism • Information warfare • System attack (e.g. distributed denial of service) • System penetration • System tampering
Industrial espionage	• Competitive advantage • Economic espionage	• Economic exploitation • Information theft • Intrusion and personal privacy • Unauthorised system access
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees	• Curiosity, ego, revenge • Intelligence • Monetary gain • Unintentional errors and omissions	• Assault on an employee, blackmail • Computer abuse, fraud and theft • Information bribery • Malicious code (e.g. virus, logic bomb, Trojan horse) • Sale of personal information • System bugs, intrusion, and sabotage • Unauthorised system access

Table 2.1: Threat sources, motivation, and threat actions (Stoneburner et al., 2002)

2.2.3 User contribution to ISR

Users are weak links to information security and over 50% of the breaches to information security originate from within an organisation (Thomson et al., 2006; Dhillon & Torkzadeh, 2006; Siponen & Oinas-Kukkonen, 2007; Steele & Wargo, 2007; Chang et al., 2009; Spears & Barki, 2010). Based on industry statistics, D'Arcy et al. (2009) account for 50% to 75% of information security incidents as perpetrated by users. These are attributed to users' unauthorised access to systems (Gordon et al., 2005), or employee noncompliance with information security policies and procedures in an organisation (Pahnila et al., 2007; Siponen & Oinas-Kukkonen, 2007; Chang et al., 2009). In some cases, information security incidents occur as a result of employees being mandated by organisational activities to circumvent fundamental information security practices in trying to have their jobs done (Bednar & Katos, 2009). The pervasiveness, penetration, and commercial success of laptops have also amplified the number of security incidents as the assumption of physical security gets challenged (Bednar & Katos, 2009). These various ways in which users contribute to information security problems highlight the gravity of the information security problems.

The percentage of information security problems originating from within organisations however does not correspond to the general corporate information security expenditure. Over 75% of corporate information security budgets are directed on protecting against outsider threats (Steele & Wargo, 2007). The budgets are spent on the acquisition of "anti-virus software, firewalls, intrusion detection and prevention systems, anti-spam, logical and physical access control systems, malware (spyware) protection, email and database encryption, and web application security systems" (Steele & Wargo, 2007). This shows that organisational efforts are mostly put on managing information security incidents from external sources at the expense of those from within. It is important to have information security budgets that are proportional to the magnitude of information security problems and at the same time those that address internal threats.

Studies have shown that users can be important in protecting the information security breaches (Chang & Ho, 2006; Siponen, 2005; Spears & Barki, 2010; Stanton & Stam, 2006; Whitman, 2008). For instance, Stanton and Stam (2006) posit that user behaviour affects the security of information in a sense that if users are of good behaviour they carefully handle data and perform their duties as expected. If users are of bad behaviour, they facilitate incidences of information security breaches. It must be emphasized that it is rather difficult to achieve 100% information security (Bodin, Gordon & Loeb, 2008) because users still make mistakes (Gordon et al., 2005) and others may be negligent (Chang & Ho, 2006). User mistakes are inevitable therefore no matter how minimal it might be enterprise information will still be vulnerable to abuse. Organisational efforts to manage information security should therefore be aimed at mitigating information security breaches.

The

2.3 Organisation and information security cultures

2.3.1 Organisational culture

Organisational Culture (OC) refers to "shared beliefs and values that develop within an organisation and guides the behaviour of its members to maintain suitable patterns of social systems" (Lim et al., 2009, p. 89). The main objective of an OC is to have coordinated behaviour among members of staff in order to survive in the

dynamic and competitive environment (Denison, 1990; Schein, 1992). OC facilitates the generation of employee commitment to the organisation. An OC helps to bind employees to the organisation by defining accepted standards and rules. It acts as a control mechanism that guides and shapes employee attitudes and their behaviour (Robbins, 1989). Through an OC, management can communicate their intentions to members of staff.

2.3.2 Information security culture

A number of definitions for Information Security Culture (ISC) exist in literature. For instance, ISC is defined as the patterns of behaviour within an organisation which contribute to the protection of information (Dhillon, 1997). ISC is also defined as anything that is done in relation to information security practices (Martins & Eloff, 2002; Da Veiga & Eloff, 2010). Realizing the importance of ISC, several researchers recommend ISC to be incorporated in users' daily activities (Schlienger & Teufel, 2003; Thomson et al., 2006; Von Solms, 2000). While enterprise-level ISC influence proper use of information systems at an organisational level, arguments in literature suggest that ISC should not only be confined to organisational boundaries. An ideal ISC is suggested to also include its possible interactions with national cultures (Leidner & Kayworth, 2006). It is therefore important to understand how these cross-culture interactions influence people behaviour towards ISRM practices.

2.4 Information Security Risk Management (ISRM)

Stoneburner et al (2002, p. 1) define ISRM as "the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level". Several other authors have defined ISRM such as follows:

> *"…understanding information security requirements, establishing security policy and objectives for information security, implementing and operating controls to manage information security risks, monitoring and reviewing the performance and effectiveness of them and continuous improving"* (ISO/IEC 27001, 2005).

> *"…the overall activities, processes, and institutions for identification, analysis, control and monitoring of risks that arise in the context of information management or by using information technology"* (Jahner & Krcmar, 2005, p. 3328)

These definitions imply that ISRM involves continuously monitoring, reviewing, and improving the information security policies, activities, processes and operating controls and implementing new information security controls in order to maintain the integrity of enterprise information.

The Information Systems and Control Association (ISACA) also define ISRM as a process of identifying vulnerabilities and threats to the information resources that belong to an organisation. ISRM involves deciding on countermeasures which reduce risk to a level that is acceptable to the organisation which is also referred to as risk mitigation. It is a continuous process involving identification as well as monitoring of information security controls that address those risks. ISRM enables IT Managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support organisation's missions (Stoneburner et al., 2002, p. 4). The main concepts in these definitions of ISRM include the identification or determination of risks to information resources, the identification of countermeasures which reduce or mitigate the risks to the level considered as acceptable to the organisation and the monitoring of the performance of the existing countermeasures. These three themes form the three core processes of ISRM named as Risk Assessment, Risk Mitigation and Monitoring and Assessment (Stoneburner et al., 2002) presented in Figure 2.2.

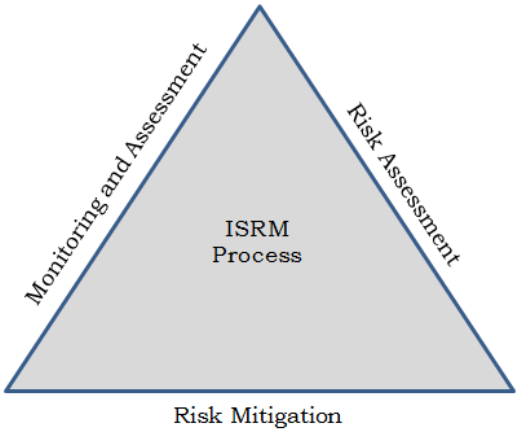

Figure 2.2: ISRM Process (Stoneburner et al., 2002).

(a) Risk Assessment

Risk assessment helps to determine the extent of the potential threat and the risk associated with an IS asset. It is used to identify appropriate information security controls for reducing or eliminating risk during the mitigation process. Information security controls are countermeasures which are planned to mitigate the likelihood that a threat exploits certain vulnerability, hence,

reducing or mitigating the risks to the level acceptable to the organisation. Information security controls can either be technical such as encryption mechanisms or nontechnical controls such as security policies (Stoneburner et al., 2002). The risk assessment process involves a number of sub processes which include system characterisation, threat identification, vulnerability identification, controls analysis, likelihood determination, impact analysis, risk determination, and control recommendation (Stoneburner et al., 2002).

(b) Risk Mitigation

This involves prioritizing, evaluating and implementing the appropriate information security controls as recommended in the risk assessment process. Sub-processes under the risk mitigation process include risk assumption, risk avoidance, risk limitation, risk planning, research and acknowledgement, and risk transference (Stoneburner et al., 2002).

In risk assumption, an organisation acknowledges the existence of potential risk and continues to operate the systems or chooses to implement controls with an aim of mitigating the risk to an acceptable level (Stoneburner et al., 2002). In risk avoidance, an organisation completely avoids the risk by eliminating the cause and its consequences. A typical example of risk avoidance is forgoing some system functionality or completely shutting down the system when risk is identified. In risk limitation, an organisation implements controls that minimise the adverse impact of a threat which exploits vulnerability. An example of risk limitation is use of preventive or detective controls such as anti-spyware and antivirus software. In risk planning, an organisation develops a risk mitigation plan which prioritizes, implements, and maintains controls. In research and acknowledgement, an organisation lowers risk by acknowledging the vulnerability and identifies controls to correct the vulnerability. In risk transference, an organisation transfers the risk by using other options to compensate for loss such as insurance cover (Stoneburner et al., 2002).

(c) Evaluation and assessment

Often times, computer networks get expanded and updated, its components get changed, and software applications get replaced or updated with newer versions. In addition, personnel changes occur and information security policies change over time (Stoneburner et al., 2002). These changes imply that new risks surface. Risks previously mitigated become a concern which makes the ISRM

process to be an on-going process and always evolving. Success of ISRM program relies on senior management commitment, full support and participation of the IT technical personnel, the competence of the risk assessment team, the awareness and cooperation of members of the user community and an on-going evaluation and assessment of the IT-related mission risks (Stoneburner et al., 2002).

The most critical element of ISRM is information security awareness. Wilson and Hash (2003) define security awareness as the process of making users aware of information security risks. The aim of information security awareness is to focus user attention on security and to allow the users to recognize security concerns and respond accordingly. Literature focuses on user awareness and education when addressing the human aspects of information security. According to Bednar and Katos (2009), literature does not address issues of relevance and motivation which are some of the important human aspects information security. Bednar and Katos (2009) suggest that an ISRM system needs to accommodate end-users' information security requirements. This may imply that efforts aimed at addressing the human aspects of information security should consider human factors beyond information security requirements. One way to achieve this is by understanding the cultural influence on human behaviour such as user participation in ISRM practices.

2.4.1 User participation in ISRM

User behaviour has important implications on organisation's information security management efforts (Lim et al., 2009). Stan (2007) posits that ideal ISC highly depends on the users' information security related beliefs and values. These beliefs and values get manifested in user actions and behaviours towards ISRM practices. In order to effectively manage information security, organisations need to carefully think of ways of influencing user behaviours. One way to influence user behaviour is by having information security policies. However, well-structured information security policies become dead documents if users are not made aware of (Siponen, 2000a). Further, information security policies do not help reduce information security incidents if they are not complied with (Doherty & Fulford, 2005). It is important for users to understand their respective roles and responsibilities and be able to build work practices based on their clear understanding of these roles and responsibilities (Dhillon & Backhouse, 2000). User work practices enable the users to demonstrate a sense of responsibility. Organisations which realize the

importance of user responsibility, therefore, instil an ISC which enables the users to know their roles and responsibilities (Dhillon & Backhouse, 2000). While accountability means accepting blame for some information security incidents, being responsible means being able to take appropriate action during future information security events (Dhillon & Backhouse, 2000). An ISC in an organisation helps to instil a culture of responsibility among the users and makes them to respond accordingly to future information security incidents.

Furthermore, literature suggests an ISC in organisation which transcends both organisational and national boundaries (Dhillon & Torkzadeh, 2006; Bednar & Katos, 2009). Due to network externalities and other impediments to information security, organisations cannot be secure if ISCs are limited by organisation boundaries. Such ISCs would not guide the behaviour of users who access information from external sources through the internet. They would also not protect the organisations when customers operating from insecure environments access enterprise information through the internet.

Secondly, organisations need to establish ways of maintaining and upholding the integrity of new members to the organisations. Dhillon and Backhouse (2000) argue that a person of integrity does not always remain so. Hence users' failure to maintain their integrity due to changes in individual pressures, marital statuses, financial, and medical problems result in users' integrity being compromised. As a result of loss of integrity, over 50% of the information security incidents originate from the users within the organisation (Gordon et al., 2005; D'Arcy et al., 2009). Organisations which strategically aim at maintaining information security establish ways of maintaining user integrity. One possible way to maintaining user integrity in an organisation is by instituting informal security systems such as ISC which come free (Dhillon & Backhouse, 2000). Organisationally grounded principles and values are essential for managing information security (Dhillon & Torkzadeh, 2006)

Thirdly, culture promotes user trustworthiness (Dhillon & Backhouse, 2000). The Concise Oxford Dictionary (1999, p. 1540) defines the word "trust" as "the state of being responsible for something". Users need to demonstrate a sense of self-control and responsibility. This, together with less external control and supervision, creates mutual systems of trust amongst the users (Dhillon & Backhouse, 2000). User supervision is not feasible in organisations which span wide geographical area. Hence, user trust among members of staff acts as a unifying element (Dhillon

& Backhouse, 2000). Culture helps build user trust through shared ethics and beliefs among the members of the organisation. Through an ISC users are trusted to be responsible and to discharge their duties in accordance with the laid down information security policies without requiring close supervision (Dhillon & Torkzadeh, 2006).

Lastly, culture promotes ethicality among the users. Ethicality, according to the Concise Oxford Dictionary (1999, p. 490) refers to "a state of maintaining moral principles of conduct or informal norms of behaviour". While organisational rules can be applied to all formalized procedures, there are circumstances where there are simply no rules. For instance, there are no rules that govern Internet usage but there are working norms which have developed the syntax for internet communications. Similarly, informal norms exist in organisations which control the behaviour of users (Dhillon & Backhouse, 2000).

Considering these different characteristics of users which are culturally motivated, literature suggests the need for organisations to understand the effect of cultural differences. This would enable organisations to successfully deploy global IT solutions or effectively manage information security (Harris & Davidson, 1999; Myers & Tan, 2002; Tan, Watson, & Wei, 1995). Successful IT systems implementation in one country does not guarantee success in another country with different national cultures. In the context of ISRM, culture makes people from different cultural origins to respond differently to the same ISRM practices. One country's success of ISRM strategy does not imply success of another country for the same ISRM practice. It is necessary for cross-country organisations to consider the influence of national cultures (Chow, Kato & Shields, 1994) or human factor (Van Niekerk & Von Solms, 2010) when implementing organisation-wide information security policies in order to be assured of effective ISRM. Literature identifies three mechanisms through which culture shapes the impacts of IS (Pang, Sharma, Lederman, & Dreyfus, 2010), which have been presented in Table 2.2.

Mechanisms	**Explanation**
Social interpretation of IS	Culture shapes how social actors perceive IS, and consequently influences their willingness to adopt and use IS as well as IS's effectiveness
Response to uncertainty	Culture determines how social actors are likely to react when faced with change brought by IS implementation.
Functional Fitness	The effectiveness and appropriateness of IS functionalities vary across different organisations and cultures.

Table 2.2: Mechanisms of how culture shapes impacts of IS (Pang et al., 2010)

On social interpretation of IS, Pang et al. (2010) posit that users assign socially constructed meanings to developed software. These meanings are usually different from those of the development team (Pang et al., 2010). Culture shapes the social interpretational processes and depending on the existing culture, the same piece of technology or ISRM strategy can be interpreted differently in different countries. The same IS technology which can be viewed as "empowering or deskilling, as reducing or enlarging existing power distance and as restrictive or liberalising" (Pang et al., 2010, p. 2) may not be viewed as such in another country. Therefore, the users' interpretation of ISRM practices is critical on their willingness to accept, adopt and use it (Cabrera & Cabrera, 2002; Gobbin, 1998).

The second mechanism of how culture shapes the impacts of IS involves response to uncertainties. Culture defines the rules that influence the way people respond to change and the associated uncertainty (Johns, Murphy Smith, & Strand, 2003). Some cultures are more tolerant to uncertainties with characteristics such as open, flexible, and sociable while others are not (Cooper, 1994; Doherty & Perry, 2001). People in more tolerant cultures are expected to be more receptive to changes in ISRM practices as opposed to those in cultures that are not tolerant. User social characteristics such as "open", "flexible", and "sociable" influence their participation in ISRM practices. Users that are flexible, due to the existing tolerant cultures are expected to participate more in ISRM practices. This would contribute more to the management of information security.

The third mechanism of how culture shapes the impact of IS or ISRM relates to functional fitness. Functional fitness refers to the ability of IS or ISRM to meet the requirements of different users within specific cultures. Pang et al (2010) posit that functional misfit is a common phenomenon in cross-cultural IS transfer projects. ISRM functional misfits can therefore be expected amongst users from different cultural origins. While users in one country may consider some ISRM practices as appropriate, users in another country, with different national cultures, may regard the same as inappropriate (Pang et al., 2010). Sharing of system access details might be unethical in some countries but can be viewed as ethical in countries where national cultures promote sharing of resources. This would result in some ISRM practices turning out to be inefficient in some countries while being efficient in other countries. Cultural characteristics, therefore, need to be considered when embarking on cross-cultural IS transfer projects or when adopting cross-cultural ISRM practices. The knowledge about national cultures and how these influence

peoples' attitude and behaviour towards ISRM practices is also essential for information security management efforts that are aimed at effectively moderating multi-cultural or multi-national information security threats. This is important in the world of diversity and globalization where information security risks are evolving along different complex dimensions.

ISRM consists of many processes and practices which are largely dependent on human cooperated behaviour (Van Niekerk & Von Solms, 2010). Inadequate level of user cooperation and knowledge about information security requirements makes many information security management techniques to become liable to abuse or misinterpretation by users. Therefore, organisations need to comprehensively address the "human factor" element when managing information security (Van Niekerk & Von Solms, 2010). Literature advocates for the need for an information security culture in the organisations in order to efficiently manage information security (Eloff & Von Solms, 2000; Von Solms, 2000) as well as a culture which transcends organisational and national boundaries (Dhillon & Torkzadeh, 2006; Bednar & Katos, 2009).

According to the participation theories of buy-in, system quality and emergent interactions (Barki & Hartwick, 1989; Barki & Hartwick, 1994; Markus & Mao, 2004; Spears, 2006; Spears & Barki, 2010), user participation is suggested to contribute positively to ISRM efforts. However, the user positive contribution to information security management can be ensured through an information security culture, which makes the users to become an information security asset rather than a risk (Van Niekerk & Von Solms, 2010). Being an information security asset means users becoming part of the solution towards addressing information security breaches. Information security assets, the detailed knowledge of business processes that users possess can be essential when identifying information security risks (Spears, 2006; Spears & Barki, 2010). Risk identification is the first step of ISRM (Stoneburner et al., 2002).

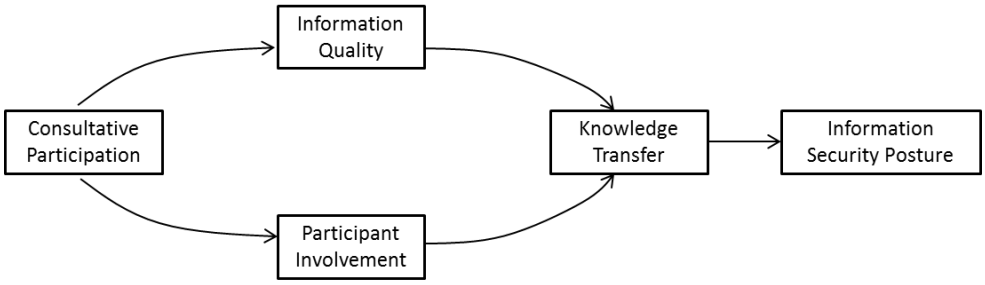

Figure 2.3: Model of Consultative Participation (Spears, 2006)

The model of consultative participation by Spears (2006) presented in Figure 2.3 theorizes the much advocated inclusion of business users in the information security risk analysis process (Suh & Han, 2003). In the model, consultative participation is expected to enhance information security posture. These are mediated by three factors: information quality, participant involvement and knowledge transfer among peers (Spears, 2006). In consultative participation, users are assigned roles and activities to perform but they do not have complete decision making authority in whatever takes place (Spears, 2006). Participant involvement is the subjective psychological state reflecting the importance and personal relevance of an object or event (Hartwick & Barki, 1994). Information quality refers to the extent to which information is complete, relevant, believable, and timely (Wang & Strong, 1996; Zmud, 1978). Knowledge transfer refers to the exchange of information between end users and information security staff while the information security posture refers to the combination of all (security policy, procedures, and technology, and ISRM projects) (Spears, 2006). If the knowledge transferred between end-users and information security staff would be used in the design and development of information security controls, the developed information security controls would be efficient (Spears & Barki, 2010).

The model of consultative participation links user participation with information security posture mediated by information quality and participant involvement. In consultative participation, users with detailed knowledge of business processes participate in information security risk analysis to identify information security vulnerabilities (Spears, 2006). The identification of unknown information security risks increases the quality of information used for ISRM. This is consistent with the system quality theory of user participation (Markus & Mao, 2004). It is expected that the increased quality of information used in ISRM would be used to design and develop information security controls that are of increased quality.

According to Spears (2006), user awareness about information security contributes to the improvement in information security development and remediation. As the users get to know more about the need and requirement of information security, they would be more willing to pass the information that they possess about business processes to information security control development staff. This information would be used to design and develop high quality information security controls. This would result in improvement in the overall information security control performance. Improvement in information security control performance implies improvement in information security management. The information that the users pass on to the information security control developers can also be used to remediate (improve) the existing controls that are identified during risk identification as weak to detect the presence of threats and prevent their impact.

There are three areas of ISRM in which end users can participate: ISRM activities, accountability roles and security control roles (Spears & Barki, 2010). These areas have been presented in Table 2.3. Control identification involves "the identification of potential threat-sources and compiling a threat statement which outlines all threat-sources that are applicable to the information resource which is currently being evaluated (Stoneburner et al., 2002).

ISRM activities	Accountability roles	Security controls
• Business process workflow • Information security control identification • Control design, implementation, testing, and remediation • Control communication	• Documenting roles and responsibilities • Assigning roles and responsibilities • Designating control owners • Security policy committee membership	• System access control • Segregation of duties • Alerts and triggers • Exception reports • End-user computing • Training • Risk tolerance

Table 2.3: User participation roles (Spears & Barki, 2010)

Control design involves development of new controls that are aimed at preventing threat-sources from exploiting the existing vulnerabilities in the information resources. Control remediation refers to the improvement to the existing controls which are identified as weak to perform their intended purposes (Stoneburner et al., 2002). The Control Objectives for Information and related Technologies (COBIT) defines controls as:

"Policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected" (Stoneburner et al., 2002, p. 20).

Having an information security policy in an organisation is just one step towards ISRM. More to it is about getting the users to know about it. User compliance with the information security policy is also an issue of concern in many organisations. Having information security policies in place does not guarantee reduction of information security incidents (Doherty & Fulford, 2005) and an information security policy which users are not made aware is a dead document (Siponen, 2000a). The other reason which makes organisations to still suffer high rates of information security incidents despite having a good policy document is its enforcement. Having an information security policy and being able to enforce it are totally different things (David, 2002). No statistically significant relationships exist between the adoption of information security policies and the number of information security incidences (Doherty & Fulford, 2005). Having realised the need for compliance with information security policies, universities seek measures such as self-regulations, staff/student handbooks, and public relation campaigns. These make members of staff and students to become aware of the information security policies. Failure of which may result in financial loss or damage to reputation (Kyobe, 2010).

Information security controls that are often associated with users in many organisations, include segregation of duties, and access control (Spears & Barki, 2010). Segregation of duties is an internal control that prevents or detects errors and irregularities by assigning responsibility for initiating and recording transactions and custody of assets to separate individuals. Segregation of duties prevents one user from initiating and completing a task in a business process cycle. This, in a process, prevents fraud and error by preventing conflict of interests of a particular user which results in breach of security (ISACA, 2008).

In addition to access control and segregation of duties, users are also involved in enacting exception reports and definition of security alerts. Exception reports are used to signify potential problems in a particular application based on pre-defined conditions (ISACA, 2008) while accountability is a security goal that generates the requirement for actions on an entity to be traced uniquely to that entity. Accountability supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. Accountability is described as responsibilities assumed by users when they are assigned tasks and roles which aim at safeguarding information assets. Accountability roles continuously keep the users informed of what the organisation expects from them.

Typical examples of such tasks include approving routine access control, data custodianship, access control specialist, and data owner responsibility (Spears & Barki, 2010).

Access control as one of the ISRM practices ensures that users have access to information resources in accordance with the defined security control policies (ISACA, 2008). The effectiveness and strength of access controls depends on the correctness of the access control decisions. Data custodians are individuals who design, develop, and operate the data warehouse (Giannoccaro, Shanks, & Darke, 1999). The data custodianship role ensures that data is accessed and used only for the intended purposes. Data owners (consumers) are those who use the data in their work activities.

The above discussion about user participation in ISRM shows that user behaviours have an important role in ensuring the efficient management of information security. This finding from literature was further examined in this study by testing the hypothesis

> ***H1: User participation in ISRM contributes to effective information security management***

2.4.2 National culture and ISRM practices

While argued not to hold after over 30 years, Hofstede's conceptualisation of national culture is popularly used in IS discipline (McCoy, Galletta & King, 2005). Hofstede (1980, p. 260) defines culture as "the collective programming of the mind which distinguishes the members of one human group from another". This definition and many others rely on the assumption that individuals' membership in cultural groups defines the nature of values that the individuals espouse. This may not always be true since an individual's values can be influenced and modified by the individual's membership in other professional organizations, ethnic, religious and various social groups (Straub et al., 2002). This suggests the inappropriateness of the assumption of homogeneity "particularly if the national culture construct is to be integrated into IS models that reflect individual behaviour.

Contrary to IS models, integration of national culture constructs into ISRM models justifies the assumption of homogeneity. Information security management is not only a matter of technology but also people management which is influenced by culture (Asai, Siripukdee, Waluyan & Noguera, 2009). According to Hofstede (1980),

culture influences people's beliefs and expectations which may lead to information security breaches. For instance, Schneier (2008) and Komatsu (2008) posit that people's expectations may be one of the causes of misjudgement on how to react to information security incidents. It is therefore natural to think that culture influences people's behaviour especially in cross-cultural environments (Asai et al., 2009). Chow et al. (1994) also posit that the behaviour and attitude of people over same management practices varies with national culture.

On another perspective of national culture, regions aim at harmonizing telecommunications policies across member states through development of regional model policies which member states can use to develop their national policies. According to the complex adaptive systems theory (Axelrod & Cohen, 2000), adaptive policies can be generated through adaptive policymaking processes which would enable rapid response to technological change. According to PREM (2010), regulation needs to take technology into account since openness to trade brings in new technologies hence new changes. Changes to the existing systems environment (e.g. expansion in network connectivity, introduction of new technologies) call for information security professionals to identify and assess new potential risks (Stoneburner et al., 2002). The new potential risks call for a review of information security management strategies which may result in new information security controls being developed or existing ones requiring remediation in order to safeguard their IT systems.

A part from harmonizing telecommunications policies, Regional Economic Communities (RECs) such as the European Union (EU), the Southern African Development Community (SADC), and the Association of South East Asian Nations (ASEAN) also need to foster member states integration through ISRM policy harmonization. This would instil information security culture among regional member states. There is lack of policy harmonization in RECs such as Southern African Development Committee (SADC) is evidenced by different member states acting in isolation. South Africa enacted the ECT act in 2002 with an aim of regulating and protecting electronic transactions (Kyobe, 2009; Michalsons, 2005) while Malawi's current Communication Act of 1998 mainly focuses on regulating postal and broadcast services (Manda, 2010) and Zimbabwe is in the process of putting together a new ICT policy which is aimed at overhauling the old ICT policy which was drafted in 2005 (Moyo, 2012). Lack of coordinated efforts in the management of information security would result in increased cross-border cyber-

attacks. Wang and Kim (2009) establish that coordinated efforts in information security management reduce cyber-attacks originating from other countries by 16 to 25%.

The danger of different cultures on implementing coordinated information security management strategies is that people in different countries may view and perceive the coordinated information security management efforts differently. While users in some countries may regard some information security concerns as appropriate and requiring action, users in other countries may regard the same information security concerns as inappropriate due to differences in their cultural characteristics. This would result in RECs member states having different information security management strategies and acting in isolation. Member states with weak information security management strategies would provide good grounds for information security perpetrators to operate from (Wang & Kim, 2009). Cultural characteristics which influence user behaviour (hence participation) towards ISRM, therefore, need to be understood in order to have effective coordinated information security management efforts.

Differences in user participation in ISRM practices may be attributed to factors such as socio-economic conditions and government ICT polices (Brown, Hoppe, Mugera, Newman, & Stander, 2004) as well as attitudinal and behavioural factors (Tan & Teo, 2000). However, national culture, as discussed above, may also be one important factor that influences user participation in ISRM practices. Culture, according to Hofstede (1980), influences user attitude and behaviour. Therefore, culture can be suggested as one of the factors attributed to the differences in user participation in ISRM between countries. This study further examined this cultural influence on user participation in ISRM between the two countries by testing the hypothesis

> **H2*: User participation in ISRM practices is the same in South Africa and Malawi***

2.5 Research contextualisation

This study was a comparative of South Africa and Malawi aimed at understanding how user participation in ISRM contributes to the management of information security. Studies have shown that people from different cultural background demonstrate different attitudes and behaviours towards ISRM practices (Chow et al., 1994; Harrison, 1992). This would have been expected for South Africa and

Malawi which have experienced post-apartheid culture (Oosthuizen & Bhorat, 2004) and a 31-year of autocratic rule (Forster, 1994) respectively. This is important as it would establish the grounds to base interdependent information security management efforts amongst countries (Wang & Kim, 2009) which would deter information security threats globally.

2.6 Lessons learnt from literature review

The literature review demonstrated that national cultures influence user attitude and their behaviour towards ISRM practices. Differences in national cultures are reflected in the different user attitudes and participation in ISRM practices. These subsequently yield different outcomes on the overall management of information security. Literature highlights the need to have ISC instilled which transcends both organisational as well as national boundaries as a way of promoting responsibility, integrity, trustworthiness, and ethicality among the users in the organisations (Dhillon & Backhouse, 2000).

The literature review recommends organisations to take an effort to understand national cultures of the countries that they conduct business with if they are to be assured of successful information security management strategies and policies. This is also true for organisations that aim at deploying global IT solutions. Successful implementations of IT solutions depend on user participation which is a reflection of national cultures. The literature review also demonstrated the need for interdependent ISRM efforts. Interdependent information security helps governments to deter cyber-attacks which originate from other countries.

2.7 Conceptual model

A conceptual model is a set of propositions or statements which represent relationships among constructs (Finne, 2000). The study was guided by the conceptual model presented in Figure 2.4. The model reflects three domains: Information Security Culture (ISC) elements, its outcomes, and reflective or underlying factors. While Spears and Barki (2010) mainly focused on user participation roles in ISRM, Lim et al. (2009) identify ISC elements which were integrated into the conceptual model (Figure 2.4). This study not only focused on understanding how user participation in ISRM practices contributes to the efficient information security management but also attempted to understand how national culture influences user attitude and behaviour towards ISRM practices. In addition, the ISC elements are latent variables which can only be assessed through

their observable behaviours and factors. Together, the ISC elements result in ISC outcomes which were measured using the reflective factors.

Data collected in the study was used to assess whether ISC existed in the respective organisations for the study participants. For instance, to ascertain that ISC existed, participants were expected to provide information which was indicative of user participation, commitment, motivation, and awareness about organisational information security management. This was based on Lim et al. (2009) who posit that users within an organisation with fully instilled ISC undergo periodic information security training programmes or awareness campaigns. ISC provides users with a sense of ownership to the information security practices. ISC makes the users to feel responsible and become committed towards information security. The users also know what to do, who to report to when faced with information security problems (Lim et al., 2009).

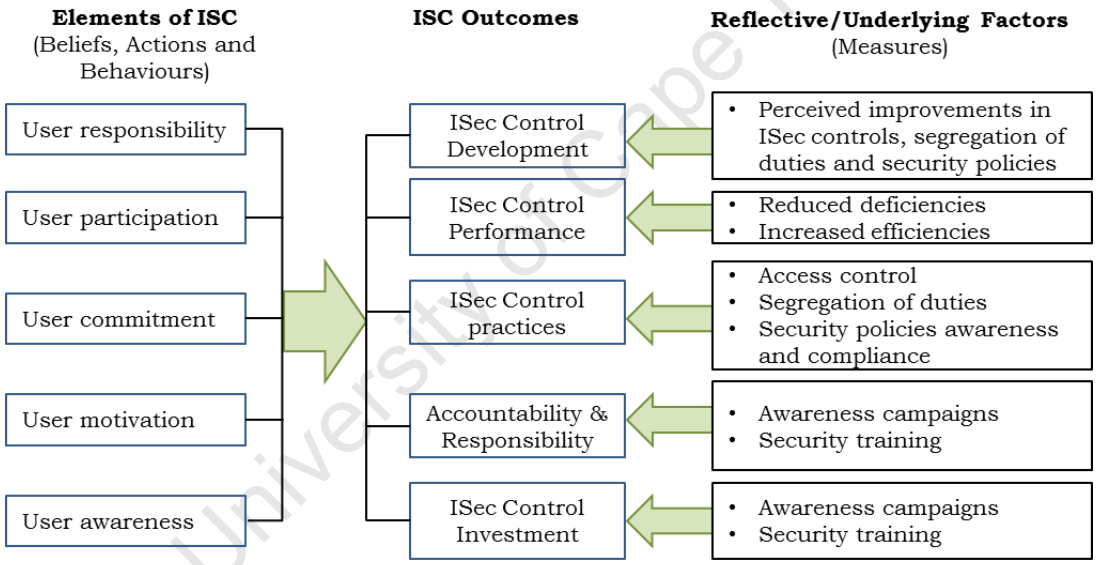

Figure 2.4: Conceptual Model (Spears & Barki, 2010; Lim et al., 2009)

2.7.1 Behavioural characteristics of ISC

Many researchers have highlighted the importance for organisations to understand and instil an ISC (Oost & Chew, 2007; Schlienger & Teufel, 2003; Thomson et al., 2006; Von Solms, 2000; Vroom & Von Solms, 2004). For instance, Von Solms (2000, p. 618) suggests "a culture of information security to be created in a country by instilling the aspects of information security to every user of ICTs as a natural way of performing his or her daily job". In addition, Schlienger and Teufel (2003) call for security culture to be instilled in organisations to support all daily activities. Vroom and von Solms (2004) as well as Thomson et al. (2006) also

recommend that ISC is an important factor in ensuring the efficient management of information security.

There are three elements of ISC which are beliefs, actions and behaviour. In relation to information security, these elements are observed in five different user-centric behavioural factors of responsibility, participation, commitment, motivation, and awareness (Lim et al., 2009). These behavioural factors were used to formulate the conceptual model presented in Figure 2.4.

a) Responsibility

As it can be noted from the conceptual model (Figure 2.4), user responsibility is the first observable characteristic of ISC. The Concise Oxford Dictionary (1999, p. 1220) defines responsibility as "the ability to act independently and take decisions without authorization". Users that are responsible have the ability to handle and act accordingly when information security incidents occur (Dhillon & Backhouse, 2000). New circumstances which may arise require users to take charge of them and act appropriately. The questionnaire consisted items which required the study participants to provide information which was reflective of the users' accountability and responsibility.

b) Participation

The second observable characteristic of ISC as reflected in the conceptual model in Figure 2.4 is user participation. Spears and Barki (2010) suggests three areas of user participation concerned with the management of information security. User participation in ISRM process activities include activities that users perform as part of the ISRM process. Users also perform routine activities that are part of information security control. The third area of user participation is through accountability roles (Alberts & Dorofee, 2003). These three areas which constitute user participation are simply formative indicators (Jarvis, MacKenzie, & Podsakoff, 2003).

c) Commitment

Drawn from the conceptualization of commitment from social exchange, marriage and organisations (Cook & Emerson, 1978; Meyer & Allen, 1984; Thompson & Spanier, 1983), Morgan and Hunt (1994) define relationship commitment as exchange beliefs where each partner believes that an on-going relationship with the other is so important as to warrant maximum efforts at

maintaining it. In the context of information security management, committed users realize the need for information security management and believe that it is worth taking part to ensure that it endures indefinitely. When commitment and trust are both present, they produce outcomes that promote efficiency, productivity, and effectiveness. Commitment and trust lead directly to cooperative behaviours that are conducive to relationship marketing success (Morgan & Hunt, 1994).

d) Motivation

The study of motivation involves asking "why people initiate, terminate, and persist in specific actions in particular circumstances" (Markus & Kitayama, 1991). A response to this question is based on some type of internal, individually rooted need or motive. The motive can be to enhance one's self-esteem, to achieve, to affiliate, to avoid cognitive conflict, or to self-actualize. These various types of motives are assumed to be part of the unique, internal core of a person's self-system (Markus & Kitayama, 1991). While no particular items were precisely structured to assess users' observable characteristics of motivation towards information security management, items which measured user accountability and responsibility, were closely related to user motivation.

e) Awareness

Information security awareness is "a state that is reflected in the behaviour of the target groups such as users (Spears & Barki, 2010). It is associated with a raised consciousness (Dinev & Hu, 2007) and an increased adoption of information security policies and countermeasures (Tsohou, Kokolakis, Karyda, & Kiountouzis, 2008). Two elements are reflective of increased user awareness about information security and these are:

a. heightened awareness of policies, procedures, and need for information security

b. users demonstrated sense of ownership in maintaining information security

2.7.2 ISC outcomes

The conceptual model reflects five ISC outcomes: information security control development, information security control performance, information security control practices, accountability and responsibility, and information security investments (Lim et al., 2009). ISC outcomes are possible consequences that

organisations face depending on the level of integration of ISC and OC. Fitzgerald (2007) classifies levels of integration of ISC and OC into high, moderate and low as presented in Table 2.4.

Class	Risk vulnerability	User security awareness	Security responsibility	Security practices	Investment
High	Low	Highly aware and concerned about security matters	Every user's business	Holistic manners, daily routine activities	High cost in security practices
Moderate	**Moderate**	Aware of security matters within their own dept.	users responsible for security matters	Users routine activities in own dept.	Medium cost in implementing sec. activities
Low	High	No awareness in security matters	Only IT dept. is responsible for security matters	Not a routing activity of users	Low cost in implementing sec. activities

Table 2.4: ISC and OC integration characteristics (Fitzgerald, 2007)

High level of ISC and OC integration refers to a state where ISC is fully embedded in OC (Fitzgerald, 2007; Schlienger & Teufel, 2003; Von Solms, 2000). High level of integration of OC and ISC results in organisations having a number of attributes: lowest information security incidents originating from the users, high information security costs (Lim et al., 2009), high integrity, responsible, trustworthy and ethicality of users (Dhillon & Backhouse, 2000) who are information security cautious. This is different from both moderate and low level of integration as it can be noted from Table 2.4.

2.7.3 Underlying or reflective factors

The conceptual model presented in Figure 2.4 also shows observable characteristics which are indicative of the ISC outcomes. For instance, the model shows three underlying factors which are reflective of information security practices. These, among many others include access control, segregation of duties and compliance with information security policies (Spears & Barki, 2010; Lim et al., 2009). Survey participants were asked to indicate whether users in their respective organisations participate in these reflective factors.

2.8 Chapter summary

This chapter has discussed the concept of user participation and also identifies the three user participation theories: buy-in, system quality, and emergent interactions theory, which explain the concept of user participation and how this influences quality and success of the information system developed. The chapter also

introduces the reader to the concepts of OC and ISC which build the base for subsequent discussion of information security and ISRM. The chapter also discusses the two images of users in the context of information security. The study context as well as the conceptual model is also presented in this chapter.

Chapter 3 : Research design

This chapter outlines the research design employed in the study as follows:

Chapter 3 is organized into five sections. Section 3.1 revisits the problem statement, research questions, research aims and objectives, and the research methodology. Section 3.2 discusses the philosophical assumptions that guided the way in which the study was conducted. Section 3.3 outlines the research methodology which in it are discussions pertaining to the purpose of the study, type of investigation employed, research method, a description of the participants, sampling method, survey instruments, data collection and analysis. Section 3.4 presents the time frame in which the study was conducted as well as the deliverables expected. Section 3.5 highlights the ethical considerations, which were which guided the conduct of the researcher.

3.1 Introduction

The previous chapter outlined two main problem areas. Firstly, there are contradicting views about how user participation in ISRM contributes to the management of information security. Secondly, studies which focus on understanding cultural influence on user behaviour (participation) towards ISRM practices are rare. To address these problems, two research questions were used to guide the study: how user participation in ISRM contributes to the efficient management of information security and how the effect of user participation in ISRM varies across nations of different cultural origins. A mixed research approach was deemed appropriate where both quantitative and qualitative methods were employed to collect, analyse and interpret data.

3.2 Philosophical assumptions

One way to classify research is to distinguish between the philosophical assumptions that guide the research (Myers, 2009). A research philosophy is a set of beliefs that guides the way of conducting research (Guba, 1990). The most pertinent philosophical assumptions in the field of IS relate to epistemology (Myers, 2009, p. 35). Epistemology is defined in the Concise Oxford Dictionary (1999, p. 480) as “the theory of knowledge”, especially with regard to its methods, validity and scope and also as the assumptions about knowledge and how it is acquired (Hirschheim & Klein, 1992).

While some authors suggest three research paradigms: positivist, interpretive, and critical (Chua, 1986; Myers, 2009; Orlikowski & Baroudi, 1991), others identify four paradigms: positivism, post-positivism, critical theory and constructivism (Guba & Lincoln, 1994) or post-positivism, constructivism, and advocacy (participatory), and pragmatic (Creswell, 2009). This varied classification of epistemologies is dependent on the discipline under study, beliefs held by the advisers and the faculty under which a particular research belongs (Creswell, 2009). While the three-fold distinction of epistemologies is just one of the many classifications, it has widely been embraced in IS literature (Klein & Myers, 1999; Myers, 2009; Ngwenyama & Lee, 1997; Richardson, 2007; Stahl & Brooke, 2008) hence adopted in this study.

3.2.1 Positivist research

Positivist studies are founded on the "existence of a priori fixed relationships within phenomena" (Orlikowski & Baroudi, 1991, p. 5). Positivist researchers believe that "reality" exists, which can objectively be measured or observed (Myers, 2009). Positivist studies assume the existence of "cause and effect" relationships which need to be identified and assessed. The problems studied in positivist studies reflect the need to identify and assess the causes that influence outcomes. These cause and effect relationships are also referred to as fixed relationships (Orlikowski & Baroudi, 1991). The fixed relationships are investigated using structured instruments such as questionnaires (Myers, 2009; Orlikowski & Baroudi, 1991). Knowledge in positivist studies is based on careful observation and measurement of the objective reality. Positivists also assume the existence of laws and theories that govern the world which need to be tested, verified or refined. In positivist studies, researchers begin with the identification of theory and then the collection of data that either support or refute the theory. Necessary revisions to the theory are made before subsequent tests are made (Creswell, 2009).

3.2.2 Interpretive research

Interpretive researchers assume that "the knowledge of reality is gained only through social constructions such a language, consciousness, shared meanings, documents, tools, and other artefacts" (Klein & Myers, 1999, p. 69). Interpretive research helps researchers to get to know human thought and action in social and organisational contexts. Interpretive studies develop knowledge based on the meanings that members of the society attach to objects or things as they discover

the world (Creswell, 2009). The main aim of interpretive research is to understand rather than predict (Walsham, 2006).

The principle of	Principle suggestion
1. Hermeneutic Circle	"All human understanding is achieved by iterating between considering the interdependent meaning of parts and the whole that they form".
2. Contextualization	"Requires critical reflection of the social and historical background of the research setting, so that the intended audience can see how the current situation under investigation emerged"
3. Interaction Between the Researchers and the Subjects	"Requires critical reflection on how the research materials (or data) were socially constructed through the interaction between the researchers and participants"
4. Abstraction and Generalization	"Requires relating the idiographic details revealed by the data interpretation through the application of principles one and two to theoretical, general concepts that describe the nature of human understanding and social action"
5. Dialogical Reasoning	"Requires sensitivity to possible contradictions between the theoretical preconceptions guiding the research design and actual findings (the story which the data tell) with subsequent cycles of revision"
6. Multiple Interpretation	"Requires sensitivity to possible differences in interpretations among the participants as are typically expressed in multiple narratives or stories of the same sequence of events under study. Similar to multiple witness accounts even if all tell it as they saw it"
7. Suspicion	"Requires sensitivity to possible biases and systematic distortions in the narratives collected from the participants"

Table 3.1: Principles that guide interpretive research in IS (Klein & Myers, 1999)

From an interpretive perspective, the subjects themselves (the people) construct their own understanding and attach meanings to objects and things of the world they live in (Lee & Lings, 2008). Interpretive research is conducted under the guidance of seven principles or fundamental guidelines (Klein & Myers, 1999) as outlined in Table 3.1. Interpretive researchers seek to understand phenomena by accessing the already existing meanings that participants in the phenomena assign them (Krauss, 2005; Myers, 2009; Orlikowski & Baroudi, 1991).

3.2.3 Critical research

Critical research is to a larger extent similar to interpretive research in its epistemological assumptions (Myers, 2009). Critical researchers assume social reality is historically constituted and that it can be produced and reproduced by the people themselves. The people's ability to change their social and economic circumstances is constrained by forms of social, cultural and political domination (Myers & Klein, 2011). Critical researchers also believe that not all interpretations are given equal weight in a particular social setting. Some interpretations are preferred over others while others may be imposed by one person or a group of people (Myers, 2009). A critical research paradigm assumes that interpretations that individuals who are socially, culturally or politically powerful make are either preferred or imposed among the members in a social setting.

Myers and Klein (2011) suggest three elements of critical research: insight, critique, and transformation. Insight is concerned with interpretation. The element of critique is "concerned with critique, the genealogy of knowledge, and the social practices of control and reproduction" and that of transformation is concerned with "suggesting improvements to the conditions of human existence, existing social arrangements, and social theories" (Myers & Klein, 2011, p. 24).

There are six fundamental guidelines or principles for conducting critical research classified into two elements: critique (the principle of using core concepts from critical social theories, the principle of taking a value position, and the principle of revealing and challenging prevailing beliefs and social practices) and transformation (the principle of individual emancipation, the principle of improvements in society, and the principle of improvements in social theories) (Myers & Klein, 2011).

Based on Fitzgerald and Howcroft (1998) who demonstrate that any epistemological stance can be employed based the preferences of the researcher and more importantly based on the purpose of the research, a positivist paradigm was preferred over the interpretive and critical paradigms. This study assumed that knowledge can be discovered and verified through direct observations or measurements (Krauss, 2005; Orlikowski & Baroudi, 1991) which, in turn, characterised the study as positivist. While positivist studies are conducted usually to test theories (Myers, 2009), the aim of the study was to understand the effect of user participation in the context of ISRM as influenced by national cultures.

Closely related to epistemology is ontology. Borrowed from field of philosophy where it refers to a systematic account of existence, the term "ontology" refers to an explicit specification of a conceptualization (Gruber, 1993) or simply the nature of reality (Migiro & Magangi, 2011). Lee and Lings (2008, p. 11, 59) also define ontology as "the belief about the nature of reality". Gruber (1993) posits that only what exists in knowledge-based systems, is exactly what can be represented. From an ontological perspective, research falls into two groups: realism and objectivism (Fitzgerald & Howcroft, 1998). While realism research assumes reality exists independent of the mind, objective research assumes reality may be unconscious of its surrounding (Crotty, 1998). The ontological position adopted in this study recognizes the existence of reality which is separate from the subjective understanding of individuals (Gregor, 2002). This therefore qualified this study as realist study. This was based on the assumption that user participation in ISRM can be observed or assessed objectively and independent of the observer.

3.3 Research methodology

3.3.1 Purpose of the study

Purpose of a study contains information about the central phenomenon that is explored in a particular study (Creswell, 2009). It defines type of contribution that a study aims to make to the existing body of knowledge. Four types of contributions of studies are identified as descriptive, explanatory (analytical), predictive, and prescriptive (Sekaran, 2003).

A descriptive study identifies a set of concepts and relationships that describes some phenomena of interest. It ascertains and describes the characteristics of variables of interest. The primary motivation for an explanatory (analytical) study is to test, explain or compare phenomena (Cavana, Delahaye, & Sekaran, 2001) whereas that for an exploratory study is to discover and explore new phenomena (Myers, 2009). An exploratory study aims at providing a better insight into the problem at hand which has been a subject of very few studies. A predictive study predicts behaviour of some phenomena that is of interest while a prescriptive study aims at describing some actions to be taken to achieve a specific outcome (Cavana et al., 2001; Hussey & Hussey, 1997; Sekaran, 2003).

The objective of this study was to provide a deeper insight on the contribution of user participation in ISRM as influenced by national cultures. This objective qualifies this study as exploratory and formed the motivation or purpose of this

study. This was found to be consistent with the definition of exploratory studies (Cavana et al., 2001; Hussey & Hussey, 1997; Sekaran, 2003).

3.3.2 Investigation type

Three types of investigations which researchers can follow when conducting research include clarification, correlational and causal (Cavana et al., 2001). In a clarification investigation, the researcher attempts to acquire a clear understanding of the concepts involved in the research problem. Researchers in correlational investigation are interested in establishing the relationships between the concepts and variables. Lastly, researchers follow a causal investigation when they aim at delineating the cause of one or more problems (Cavana et al., 2001). A correlational investigation path was taken in the study. The definitive feature of positivist epistemology, as the study was characterised, is that positivists aim at investigating fixed relationships using instruments such as questionnaires (Myers, 2009; Orlikowski & Baroudi, 1991). The correlational investigation path which was used in this study was therefore consistent with the prior epistemological assumption made in the study.

3.3.3 Research method

Reliability, relevance, and quality of research results largely depend on the method that a researcher employs to conduct a particular research. A research method is defined as "a strategy of inquiry" (Myers, 2009, p. 24). Research methods generally fall into two broad classes: quantitative and qualitative (Onwuegbuzie & Leech, 2004). Quantitative research methods use mathematical and statistical tools that are used to identify facts and relationships amongst constructs within an area of study (Fitzgerald & Howcroft, 1998). Quantitative studies are conducted through surveys (questionnaires), experiments or through mathematical modelling (Myers & Avison, 2002). Contrary to quantitative methods, qualitative research methods are used to study the environment, situations and procedures that cannot be interpreted quantitatively (Myers, 2009). Qualitative research methods make it possible to have an in depth study of human behaviour through involvement with the respondents. Typical examples of qualitative research methods include focus group discussions structured and semi-structured interviews.

There have been on-going debates regarding the appropriate methods for conducting research (Onwuegbuzie & Leech, 2004). The arguments have been to either adopt a single line of methodology or to have a combination of both

quantitative and qualitative research approaches (Onwuegbuzie & Leech, 2004). Both quantitative and qualitative purists, view their paradigms as ideal for conducting research. This, in some way, advocates for the "incompatibility theory" (Howe, 1988) which posits that these two paradigms cannot be mixed. Representing his qualitative purist position, Guba, (1990, p. 81) contends that "accommodation between paradigms is impossible". On the contrary, the goal of mixed methods, as Johnson and Onwuegbuzie (2004) suggest, is not to replace either of the quantitative or qualitative approaches but rather to benefit from the strengths and reduce the weaknesses of each of these research paradigms. Mixed methods approach enables researchers to have a broader and complimentary view of the area being researched (Collins & Hussey, 2003). In addition to this goal, research today is becoming "increasingly interdisciplinary, complex, and dynamic" (Johnson & Onwuegbuzie, 2004, p. 15). It is therefore necessary for researchers to complement one method with another. This demands researchers to understand multiple research methods which would facilitate communication and promote collaboration thereby providing research that is of high quality (Johnson & Onwuegbuzie, 2004).

The widespread acceptance of mixed methods research approach has however been limited by debates such as the paradigm method and the "best" paradigm issue (Migiro & Magangi, 2011). There have been debates as to whether the philosophical assumptions and the research methods need to be fitted together or not. For instance, paradigm differences can be identified in terms of epistemology (how people know what they know), ontology (the nature of reality) and axiology (the place of values in research) and methodology (the process of research) (Guba & Lincoln, 1988). In response, Reichardt and Rallis (1994) argue that a post-positivist philosophical paradigm can be combined only with quantitative methods and that an interpretive paradigm can be combined only with qualitative methods. This perspective leaves the mixed methods untenable because certain paradigms and methods could not "fit" together legitimately.

The "best paradigm" issue demands the philosophical paradigm which can be considered as the best foundation for mixed methods research. The debate surrounding the "best paradigm" issue maintains the perspective that mixed methods research allows researchers to use any number of philosophical foundations for its justification and use. The best paradigm to be employed in a particular study is determined by "the researcher and the research problem not by

the method" (Migiro & Magangi, 2011, p. 3758). Considering the problem in this study, epistemologically stance was considered to be epistemologically appropriate as well as a mixed methods approach as the research method.

Reasons for using mixed methods research go beyond the notion of triangulation (testing the consistency of findings obtained through different instruments) (Migiro & Magangi, 2011). With mixed methods research, results acquired from using one method are used to elaborate on results acquired from using the other method. This is referred to as complementation (Migiro & Magangi, 2011). Mixed methods research also allows for different methods to be used for different purposes in a study. A typical example is use of interviews to get a feel for key issues before embarking on a questionnaire survey. Mixed methods research also enables triangulation to take place. Migiro and Magangi (2011, p. 3759) define triangulation as "the use of different data collection methods within one study in order to ensure that the data are telling you what you think they are telling you". The mixed methods approach also helps to explain on quantitative results with the subsequent qualitative data. Lastly, qualitative data collected in mixed methods research can be used to develop theory that can subsequently be tested using the quantitative data (Migiro & Magangi, 2011).

Aspects that are considered when designing and planning mixed methods research: timing, weighting, mixing and theorizing or transforming perspectives (Creswell, 2009). Mixed methods researchers need to decide on whether the quantitative and qualitative data collection will be in phases (sequentially) or gathered at the same time (concurrently). In phased data collection plan, either quantitative or qualitative data collection can come first. Data in this study was collected concurrently. The time when invitations to complete the questionnaire were sent to the survey participants, semi-structured interviews were being conducted in Malawi. Some of the questions on the questionnaire were also structured to solicit qualitative data from the survey participants. This ensured concurrent collection of both qualitative and quantitative data.

Weighting or priority is the second factor that goes into the design procedures for mixed methods research (Creswell, 2009). In view of the purpose of the study (correlational), which can only be measured or assessed quantitatively, more weight was put on the quantitative data than on qualitative data. There was more interest in acquiring views and perceptions relating to user participation in ISRM from a

larger population of information security administrators and information systems auditors. The qualitative data was mainly used to define user participation roles in ISRM. While the survey questionnaire also captured this type of information, a clear picture of user participation roles in ISRM was acquired through the semi-structured interviews.

In mixed methods research, mixing of the two types of data takes place at different levels: the data collection, the data analysis, interpretation or at all three phases (Creswell, 2009). Mixing of data in mixed methods research means either the qualitative and quantitative data are merged on one end, kept separate, or combined in some way (Creswell, 2009). The survey instrument (the questionnaire) was used to collect both quantitative and qualitative data (mixing at data collection). During data analysis and interpretation, reflective indicators of user participation in ISRM (qualitative in nature) were used in the validity and reliability analyses and the interpretations thereof (mixing at analysis and interpretation). Mixing of the data types in this study was therefore performed at all the three stages (data collection, analysis and interpretation).

The mixed methods research approach was consistent with the epistemological positivist assumption which recommends structures such as questionnaires to be used to study and establish the "cause and effect" relationships (Myers, 2009; Orlikowski & Baroudi, 1991). Questionnaires were used to solicit ideas and suggestions from a larger population about the contribution of user participation in ISRM, as influenced by culture, on the management of information security. Concepts and ideas collected through semi-structured interviews were used to confirm those collected quantitatively through the survey questionnaire (Cavana et al., 2001).

3.3.4 Study population

Participants to the survey included those having a bias towards information security such as IS auditors and information security administrators. The responsibilities of information security administrators are "to ensure that various users within an organisation comply with the corporate security policy and that information security controls are adequate to prevent unauthorised access to data, programs and equipment" (ISACA, 2008, p. 109). Among many others, the functions of information security administrators include maintaining access rules to data and IT resources; maintaining security and confidentiality over issuance

and maintenance of user IDs and passwords; monitoring security violations and taking corrective actions, reviewing and evaluating the information security policy and suggesting necessary changes to management; preparing and monitoring the information security awareness programs for all employees within an organisation; and testing the security architecture to evaluate the security strengths and detect possible threats (ISACA, 2008). Information security administrators were, therefore, an ideal group of professionals which was expected to provide the best assessment as to the roles assumed by users as part of information security practices in various organisations.

Secondly, IS auditors are individuals who regularly "review and evaluate automated information processing systems, related nonautomated processes and the interfaces between them" (ISACA, 2008, p. 27). According to ISACA (2008), IS auditors provide an assurance to management that information systems and related resources

> "*…adequately safeguard assets, maintain data and system integrity and availability, provide relevant and reliable information, achieve organisational goals effectively, consume resources efficiently and have in effect, internal controls that provide reasonable assurance that business, operational and control objectives will be met and that undesired events will be prevented, or detected and corrected, in a timely manner*".

IS auditors were also considered suitable to provide an objective account of roles and responsibilities that users assume in various organisations as part of information security management.

3.3.5 Sampling

Quality of a social research can be assessed based on four criteria: authenticity, credibility, representativeness and meaning (Scott, 1990). Authenticity is concerned with the originality of the evidence gathered. Credibility is concerned with the evidence being free from errors and distortion. Meaning is concerned with clarity and comprehensibility of the evidence and representativeness is concerned with the typicality of the evidence (Myers, 2009). Myers (2009) further defines representativeness as the extent to which a sample can be taken as representative of a population from where the sample was chosen. It is the extent to which findings, characteristics, or lessons learnt from observing a sample would represent

those of the larger population. The question of representativeness inherently deals with the sampling technique employed in a study.

3.3.5.1 Quantitative sampling and strategy

The technique used to identify participants to the survey in both South Africa and Malawi is what is referred to as snowball sampling (Coleman, 1958). In snowball (also known as chain-referral) sampling, participants recruit their friends (Biernacki & Waldorf, 1981; Salganik & Heckathorn, 2004) hence snowball sampling is also referred to as respondent-driven sampling method. The technique starts by identifying a few participants who, upon being interviewed, the respondents refer the researcher to their friends as potential participants who possess the desired characteristics (Cavana et al., 2001; Goel & Salganik, 2010). Snowball method was originally developed to overcome problems of sampling in the studies of hidden populations.

One problem associated with snowball method is that it is not possible to determine sample representativeness. It is therefore not possible to make generalisations from studies which use snowball sampling method (Goel & Salganik, 2010). The other problem associated with snowball sampling method is that the method is strongly biased (Faugier & Sargeant, 1997). In snowball sampling, individuals having many inter-relationships have high chances of being included in the sample and snowball samples lack individual inclusion probabilities (Faugier & Sargeant, 1997). This consequently makes it impossible to have unbiased estimations, which is the case with probabilistic sampling methods such as simple random sampling method.

While the weaknesses of snowball sampling were appreciated, the method is recommended in literature (Faugier & Sargeant, 1997; Snijders, 1992), as the appropriate way to reach populations which are difficult to contact (hidden population). The method is also suggested as a formal method intended to make inferences regarding populations of individuals. Snowball sampling technique is highly recommended for studies where no member groups, lists, or identifiable clusters exist for the target population (Cavana et al., 2001; Faugier & Sargeant, 1997; Snijders, 1992). This was the case in Malawi where no forums or local chapters for information security professionals or IS auditors existed at the time of conducting the research from where participants to this study which would have

provided a sampling frame where participants to the study could have been identified.

While the question of representativeness is highly considered as the greatest weakness of snowball sampling method (Cavana et al., 2001; Faugier & Sargeant, 1997; Hendriks, Blanken, Adriaans, & Hartnoll, 1992), it is also suggested in literature that the distribution, size and type of people in the snowball sample would account for some level of representativeness (Faugier & Sargeant, 1997). These would make some degree of statistical inference possible. These arguments show more strengths of the snowball sampling method than its weaknesses. Its use in this study was therefore deemed appropriate while at the same time being mindful of the weaknesses as discussed above.

3.3.5.2 Sampling strategy for the qualitative study

In Malawi, Blantyre Water Board (BWB) was selected through simple random sampling or unrestricted method (Sekaran, 2003). Simple random sampling is a technique of identifying participants to a study where "every element in the population has a known and equal chance of being selected as a subject" (Sekaran, 2003, p. 270). BWB was randomly selected from a list comprising of six (6) water supply companies and four (4) mobile telephone service providers as listed in Appendix E. Utility companies were chosen as they are geographically found in all the three regions of Malawi.

Interview participants were subsequently selected purposively from BWB. Purposive sampling involves obtaining information from specific members of the target population who can specifically provide the information that is desired in a study (Sakaran, 2003). An interview is a data gathering technique that involves questioning the subjects that are referred to as informants or interviewee (Myers, 2009). There are different types of interviews: structured, unstructured and semi-structured. In structured interviews, the interviewer has a list of predetermined questions which are administered by telephoning, personally or through a computer. In structured interviews, the information to be collected is known at the outset (Sekaran, 2003). In unstructured interviews, the interviewer does not have a planned sequence of questions that are to be asked. The main aim of unstructured interviews is to bring to the surface issues that need further investigation (Sekaran, 2003). In semi-structured interviews, the researcher has preformatted questions to be asked and based on the respondent's answer; the researcher may ask other

relevant questions. This is a combination of unstructured and structured interviews (Sekaran, 2003). The semi-structured interview type was adopted in this study.

3.3.6 Survey instruments

Two study instruments were used to collect data. An interview guide (Appendix A) was used to collect data from semi-structured interviews and a questionnaire (Appendix B), was used to collect data from the survey participants. A questionnaire is "a pre-formulated written set of questions to which respondents record their answers" (Cavana et al., 2001, p. 226). Since the instruments were adapted from Spears and Barki (2010), pre-testing of the instruments was not deemed necessary.

3.3.7 Measurement of variables

A variable is defined as "a characteristic or an attribute of an individual or an organisation that can be measured or observed" (Creswell, 2009, p. 50). Researchers in Psychology prefer to use "construct" rather than "variable" (Creswell, 2009). These terms were used interchangeably in this study. Some constructs such as blood pressure, pulse rates, temperature are easy to measure through the use of measuring instruments while others such as people's feelings, attitudes, and perceptions become difficult to measure (Sekaran, 2003). One way to measure such things is by reducing their abstract notions to observable characteristics or behaviours (Cavana et al., 2001; Sekaran, 2003) which are also referred to as dimensions.

Considering the objective of the study, i.e. to understand the effect of user participation in ISRM as influenced by OC or ISC, three concepts as presented in Figure 3.1, were of interest to be measured in the study. These include user participation, ISRM, and culture (OC or ISC).

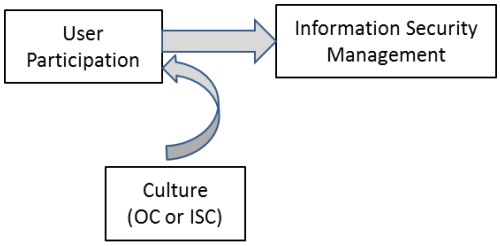

Figure 3.1: Conceptual relationships

a) User Participation

Three dimensions of an ISC include beliefs, actions and behaviour (Lim et al., 2009). As one of the variables which cannot be measured directly, user participation was measured by its observable characteristics. Participants to the study were asked to list user participation roles which are within the scope of information security management. These were then classified according to the five observable characteristics of culture: responsibility, participation, commitment, motivation and awareness (Lim et al., 2009).

b) Information Security Culture (ISC)

Literature posits that ISC influences user behaviour towards ISRM practices (Lim et al., 2009; Lim et al., 2010; Robbins, 1989). It was assumed that for users to be motivated and actually participate in information security management practices, ISC and OC must first exist in the organisation which facilitates the users' commitment, attitude and behaviour (Robbins, 1989). ISC is one example of variables which cannot be measured directly since it involves user feelings, attitude, and perceptions (Sekaran, 2003). The existence of ISC in the participants' organisations was therefore measured through the five observable user characteristics as depicted in the conceptual model (Figure 2.4). These include user responsibility, participation, commitment, motivation and awareness (Lim et al., 2009) about the management of information security.

The questionnaire survey instrument contained items which were reflective of these five observable characteristics of ISC. For instance, participants were asked to list roles which users performed in their respective organisations as part of information security management practices. The participants were also asked to indicate if users in their respective organisations show a sense of responsibility and commitment to maintaining information security. Similarly, the questionnaire contained items which captured information about user awareness about information security. This information was used to assess the existence of ISC in various organisations.

Based on the expectancy theory, user motivation, which is also referred to as "behavioural intention" (Burton, Chen, Grover, & Stewart, 1992) to use a particular system or to participate in ISRM was measured or assessed by observing the user's actual participation in ISRM. User motivation or behavioural intentions can only be measured by observing behavioural

characteristics (Creswell, 2009). Similarly, user commitment to ISRM is manifested through the users' actual participation in information security practices. Questionnaire items which were reflective of these observable characteristics of ISC were therefore the same as those for user participation in ISRM. Reflective items for user awareness about information security were measured on a five-point Likert scale.

1. Strongly agree (users often need to be reminded to follow security policy)
2. Disagree
3. Neutral (not certain)
4. Agree
5. Strongly agree (users often ask for clarification on the information security policy)

c) Information Security Management

Participants to the study were also asked to provide a list of roles performed by users in their respective organisations as part of information security management practices. Typical examples of information security management practices include granting of access, segregation of duties and compliance with information security policies as outlined in the conceptual model (Figure 2.4).

Significant differences in the data collected in South Africa and Malawi about the observable characteristics of ISC were expected to be reflective of cultural differences between the two countries.

3.3.8 Data collection

In South Africa, invitations to participate in the survey were sent to 200 registered members of ISACA through ISACA's South Africa Chapter. Out of the 200, 41 respondents responded representing a response rate of 20.5%. In Malawi, a total of 58 invitations were sent out through snowball sampling method and only 31 responses were received representing a response rate of 59.6%. In total, 72 responses were received (56.9% for South Africa and 43.1% for Malawi).

Six members of staff were purposively selected from Malawi BWB for semi-structured interviews. Of the six, one was Head of IT, one the Head of Internal Audit, three zone managers, and one Planning and Development Manager. All the semi-structured interview participants were purposively selected.

3.3.9 Data analysis

The data analysis process was preceded by the data cleaning process. Data was exported into Microsoft Excel 2010 where it was checked for incompleteness and inconsistences. For instance, some respondents had entered "2 yrs" to indicate number of years that they had been working on their position instead of just "2" as was expected. Omissions were also checked and where necessary, the data was edited. Subsequently, data was exported to IBM SPSS Statistics 20 where it was analysed.

3.3.9.1 Data description

Data was summarised and described using descriptive statistics. These include measures of central tendency and dispersion. Item means and variances were used to establish whether the questions were properly worded (Sekaran, 2003). A mean is "a measure of central tendency that offers a general picture of the data" (Sekaran, 2003, p. 396). The mean takes away the need to examine each of the observations in a data set.

Measures of central tendency do not provide enough information about the data as two data sets may have the same mean but with different dispersions (Sekaran, 2003). It is therefore important to know the variability that exists in a set of observations. Three measures of variability are range, variance and standard deviation. Only the standard deviation was used in this study as it is the most commonly used among the three (Sekaran, 2003). Measures of dispersion and central tendency help to establish whether respondents similarly respond to the questionnaire items. The measures also help to detect gaps and outliers (Hussey & Hussey, 1997). Hussey and Hussey (1997, p. 200) define an outlier as "an extreme value or item of data which does not seem to conform to the general pattern".

The frequency distributions for the demographic variables were obtained and visual displays of histograms and bar charts were produced. This helped in establishing how data for each demographic variable was distributed. Knowledge about the distribution of the data is required by some statistical tests such as the parametric tests which require some proof of the data having a normal distribution. One such assumption is, for example, the data to be normally distributed (Cavana et al., 2001; Field, 2005; Sekaran, 2003). Questionnaire item means were checked for significant difference between the data collected in South Africa and that from Malawi using Mann-Whitney U test. This is a nonparametric test which is ideal for

examining significant differences between independent sets of data (Sekaran, 2003). Non-parametric tests do not assume the data to be normally distributed.

3.3.9.2 Construct validity analysis

Construct validity analysis was used to establish whether the questionnaire tapped the concepts of user participation in ISRM just as they were theorized in this study. A statistical technique referred to as Factor Analysis is often used to identify the underlying structure of data sets (Ghauri & Grønhaug, 2002). Factor analysis is "a statistical technique used for reducing a large number of variables to a meaningful, interpretable and manageable set of factors" (Cavana et al., 2001, p. 456). The principal factor analysis was used in this study. This accounts for total variance and is used to reduce a complex set into simpler subsets. The second type of factor analysis is known as exploratory factor analysis. This accounts for common variance and is appropriate for discovering unknown structures. A part from checking for goodness of the data, factor analysis is also used to examine the validity of constructs. The factor analysis technique was used in the current study to assess whether the constructs precisely measured the concepts which they were intended to measure.

3.3.9.3 Internal consistency of measures

This measure was performed to establish whether the items under each extracted factor hanged together as a set. This was also aimed at establishing whether the items were capable of independently measuring the same concept. This was to enable deductions that respondents attached the same overall meaning to each of the items under each extracted factor. According to Sekaran (2003), internal consistency of measures is assessed by checking if the items are highly correlated.

3.3.9.4 Instrument reliability analysis

Reliability is alternatively defined as "a way of ensuring that a scale consistently reflects the construct it is measuring" (Field, 2005, p. 666), the extent to which measurements of a variable are repeatable and that any random influence which makes the measurements to be different from occasion to occasion is a source of measurement error (Nunnally, 1967), or as "the extent to which a measure is without bias (error-free) and hence ensures consistent measurement across time and across various items in the instrument" (Sekaran, 2003, p. 203). The theme in

these definitions is for a measurement to be error-free over time and in different measuring conditions.

One type of reliability measure is internal consistency measures (Sekaran, 2003). is referred to as inter-item consistency reliability. The most commonly used inter-item consistency reliability test is the Cronbach's alpha (Cavana et al., 2001; Creswell, 2009; Sekaran, 2003). Though popularly referred to as "the" estimate of reliability, Cronbach's alpha is not the only way to estimate reliability (Cortina, 1993). The choice of the method used to estimate reliability depends on the sources of variance that are considered relevant in the study. If of interest are errors associated with time, then the test-retest approach may be used to estimate reliability. If error factors associated with the use of different items are of interest, then internal consistency tests such as Cronbach's alpha becomes appropriate (Cortina, 1993). Error factors associated with the use of different items were of interest in this study hence internal consistency test using Cronbach's alpha was performed to estimate reliability.

Cronbach's alpha takes into account variances attributed to subjects and the interactions amongst the subjects and items (Cortina, 1993). It indicates how well the items in a set are positively correlated to one another (Cavana et al., 2001; Field, 2005). While many books, journals or people consider .7 and above as acceptable values for Cronbach's alpha to indicate reliable scale, empirical evidence shows that a large alpha value does not necessarily imply reliability in the scale (Cortina, 1993; Field, 2005). This is due to the fact that Cronbach's alpha is dependent on the number of items (N) that are in the scale. Cronbach's alpha is computed using the following equation:

$$\alpha = \frac{N^2 Cov}{\sum S^2_{item} + \sum Cov_{item}}$$

Where Cov = Covariance

S^2 = Variance

N = Number of items in the scale

As the number of items on the scale increases, the value for Cronbach's **α** also increases. A large value of α can therefore be obtained if one increased the number of items on the scale.

3.3.9.5 Hypotheses testing

Two hypotheses were tested in this study. The first hypothesis (H1), proposed that user participation in ISRM contributes to the efficient management of information security. In line with the type of investigation that was employed in this study, correlational associations were used to establish the relationships between various constructs.

The second hypothesis (H2) proposed that the participation of users in ISRM practices in South Africa and Malawi is the same. This was tested using the parametric *t*-test. A *t*-test is designed for testing the difference between two-sample means. There are two types of *t*-tests: independent and dependent *t*-tests. An independent *t*-test is performed when there are two experimental conditions with two different participants while a dependent (also known as paired or matched-pairs) is performed when there are two experimental conditions but with the same participants (Field, 2005). Since this study had its participants drawn from South Africa and Malawi, independent t-test was used to test the difference between the two-sample means.

The assumptions under the independent *t*-test include data normality, data measured at an interval scale, variances in the groups being equal (variance homogeneity), and the scores being independent (Field, 2005). The variance homogeneity assumption was tested using Levene's test while the normality assumption was assumed based on the Central Limit Theorem (CLT) which posits that given a distribution with a mean μ and variance σ^2, the sampling distribution of the mean approaches a normal distribution with a mean (μ) and a variance σ^2/N as N (the sample size) increases (Lumley, Diehr, Emerson & Chen, 2002). This study had 72 responses where 45 were complete and usable responses. This was considered to be reasonably large to warrant the normality assumption.

3.4 Research time frame

There are two approaches with respect to research time frame: longitudinal and cross-sectional. A longitudinal research is conducted over a long period of time while a cross-sectional research is conducted over a short period of time (Gray, 2009). This study was conducted from February to August 2012 hence characterised as cross-sectional. A detailed time plan is presented in Appendix F.

3.5 Ethical considerations

Sekaran (2003, p. 17) defines ethics in business research as "a code of conduct or expected societal norm of behaviour". Not only does ethical conduct apply to the researchers but also to the members who sponsor the research. According to Sekaran (2003), the observance of ethics in research needs to begin with the person instituting the research. It is also expected of the researchers to demonstrate a good ethical behaviour throughout the period of conducting the research.

This study ensured research ethics were observed throughout the time when the research was conducted. In line with Sekaran (2003), respondents to the survey as well as participants for the semi-structured interviews were not asked to identify themselves by names. In addition, information provided by the respondents was treated as confidential as possible. The purpose of the study was also clearly outlined to the participants through the letter of introduction herein attached in Appendix C and verbally communicated to the participants before conducting an interview. It was also ensured that no intrusive information was solicited from the participants. Also, it was clearly indicated that participation in the survey was mandatory. The interview participants were made aware of use of monitoring devices such as voice recorders before commencement of each interview. Lastly, before instituting the research, an ethics clearance was sought from the University of Cape Town Research Ethics committee for approval.

3.6 Chapter summary

There are four sections presented in this chapter. Firstly, the chapter presents the research philosophy. This reflects the way how the researcher believes knowledge is developed or acquired. Research philosophies determine the way in which a particular study is conducted. Secondly, the chapter presents the research methodology. This discusses various areas pertaining to the execution of the research which include a discussion of the purpose of the study, type of investigation, the research method, survey participants, sampling, data collection and analysis. The chapter also presents the research time frame as well ethical considerations which guided the conduct of the researcher throughout the period the study was conducted.

Chapter 4 : Data analysis and research findings

This chapter presents the data analysis results as well as the discussions for the results. The study collected both quantitative and qualitative data through survey questionnaire and interviews respectively. The chapter is organized as follows:

Section 4.1 outlines the demographic characteristics of the participants, data analysis and its interpretations. Quantitative data analysis and discussions for the results are presented in Section 4.2. In Section 4.3, results for both internal validity and reliability are discussed. Hypothetical test results are laid down in Section 4.4.

4.1 Demographic characteristics of participants

4.1.1 Educational qualifications

There were 72 participants in the quantitative study (56.9% from South Africa and 43.1% from Malawi). The response rate was 20.5% in South Africa and 53.4% in Malawi. In total, there were 24 graduates (12 from each country) representing 33.3% of the participants and 26 post graduates (9 for Malawi and 17 for South Africa) representing 36.1% of the respondents. There were also 17 participants (8 for Malawi and 9 for South Africa) representing 23.6% of the total participants who had attended some college but had no degrees and the rest had associate degrees. See Figure 4.1. With this education background, the participants were expected to provide a good assessment of user participation in ISRM practices.

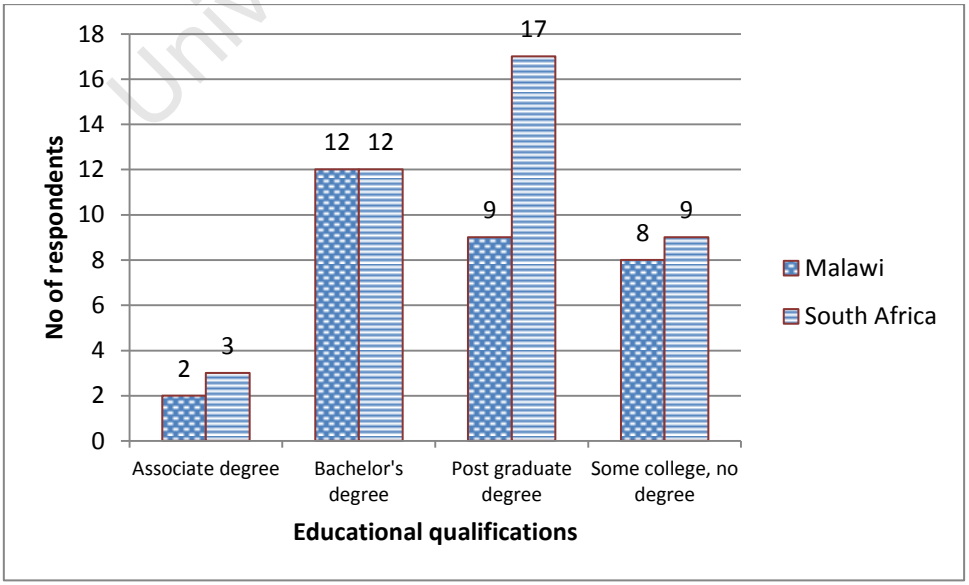

Figure 4.1: Respondents by educational qualifications

As it can be noted from Figure 4.1, there seemed to be slight differences on participants' education backgrounds between participants from South Africa and those from Malawi. While participants in South Africa mainly comprised of those holding Bachelor's degrees and post-graduate degrees, the majority of participants from Malawi were graduates from high schools and holders of post-graduate degrees. Despite these minor differences in educational qualifications, the participants from the two countries were highly educated. They were therefore expected to provide a sound assessment of user participation in ISRM practices which, in turn, contributes to the management of information security.

4.1.2 Professional qualifications

Figure 4.2 shows that about 90% of the respondents had professional certifications that were specific to information security management and information security auditing.

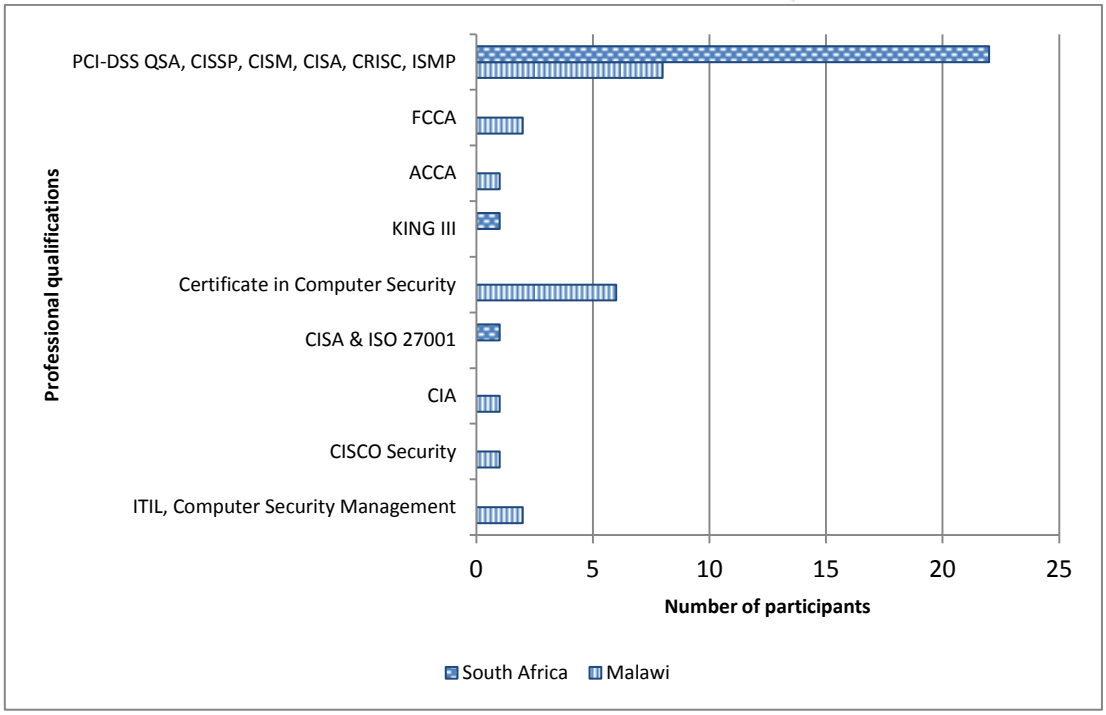

Figure 4.2: Respondents by professional qualifications

The respondents demonstrated a good command of knowledge about user participation roles in ISRM. Respondents listed user participation roles which are consistent with the ISRM practices according to Spears and Barki (2010) and Stoneburner et al (2002). All the participants were working as information security administrators, information security compliance officers, or information systems auditors. Therefore, quality and objectivity in the information provided was

expected. This had a bearing on the value and reliability of the findings from this study.

4.1.3 Industry types

For an organisation to have a risk appetite (amount of risk an organisation is willing to accept in pursuit of stakeholder value), it first needs to understand its risk profile. The number of respondents per industry types was assumed to be a reflection of the information security risk appetites for the industries. For instance, financial institutions (finance, banking, and insurance) had the highest number of respondents in Malawi while in South Africa the government and military seconded by financial institutions had the highest numbers of these professionals as can be noted from Figure 4.3.

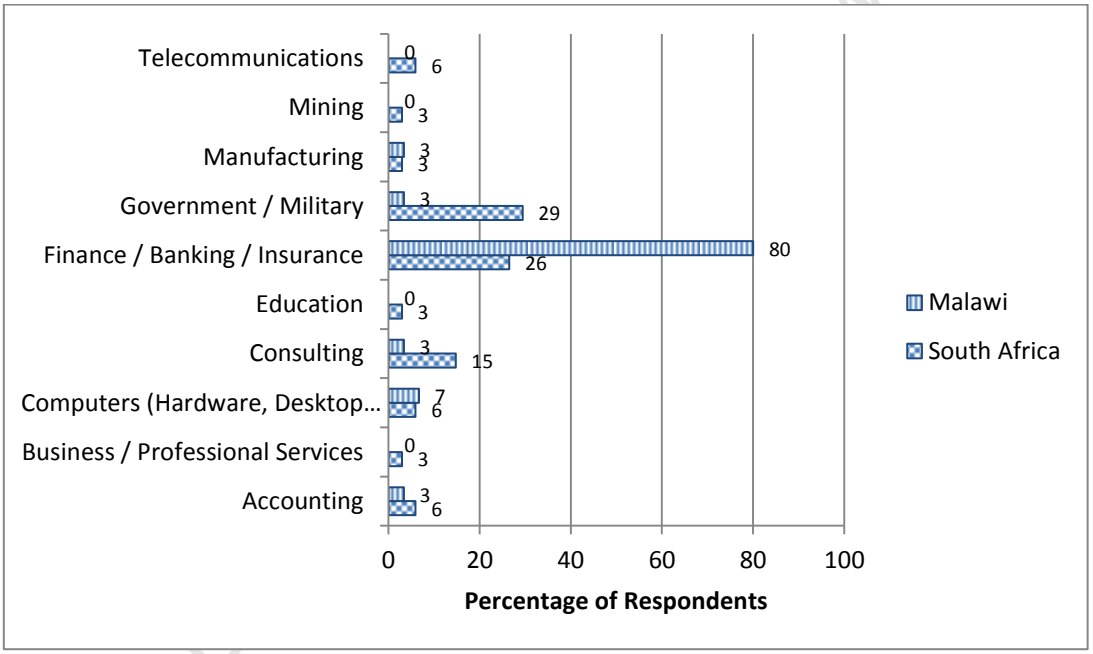

Figure 4.3: Respondents by industry types

The industries having the highest numbers of information security professionals can be concluded to be more interested in managing information security. As reflected in Figure 4.3, 70% of the respondents in South Africa came from government and military (29%), financial institutions (26%), and consulting firms (15%). These industries were, therefore, identified as having the good appetite for information security management. On the contrary, 80% of the respondents in came from financial institutions hence the only industry identified as having a good appetite for information security management in Malawi.

4.2 Quantitative methods

The quantitative methods were used to examine statistical relationships between constructs. There are three main objectives behind quantitative data analysis: describing the data (getting the feel of the data), testing for the goodness of the data, and testing hypotheses developed for the research (Sekaran, 2003). The feel for the data provides researchers with the preliminary ideas of how good the scales used in the study were and how well the coding and entering of data has been.

Testing the goodness of data involves testing for both reliability and validity of measures used in the research study. Reliability of a measure is established by testing for its consistency and stability. According to Sekarani (2003, p. 307), "consistency indicates how well the items measuring a concept hang together as a set". The Cronbach's alpha was used as a reliability coefficient which "indicates how well the items in a set are positively correlated to one another" (Sekaran, 2003, p. 307). If the computed Cronbach's alpha is closer to 1, the internal consistency (or the measuring scale) is said to be highly reliable. Hypothesis testing is achieved by using relevant statistical tests according to the type of data. Hypotheses testing aim at substantiating the predictions made in the study.

Contrary to the data analysis approaches in quantitative studies which often begin with a description of the data (Cavana et al., 2001; Sekaran, 2003), and then flowing through to validity and reliability tests, quantitative data analysis followed the plan presented in Figure 4.4. The survey instruments were adapted from Spears and Barki (2010). While instrument pre-testing was deemed not necessary, their validity and reliability were required to be checked before the actual data analysis and hypothesis testing were conducted. The subsequent data analyses were conducted based on the extracted constructs and not those reflected on the questionnaire survey instrument.

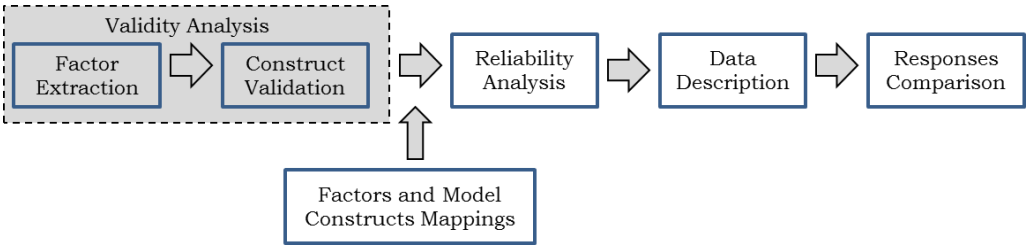

Figure 4.4: Quantitative data analysis approach

4.2.1 Validity analysis

4.2.1.1 Construct validity

As already discussed in Section 3.3.9.2, construct validity analysis was used to establish whether the survey instrument tapped the concepts of user participation in ISRM as theorized. Table 4.1 shows linear components (or factors), which were extracted at Eigenvalues greater than 1. Eigenvalues indicate substantive importance of each factor. Eigenvalues represent the amount of variation explained by a factor. This variation is also expressed as a percentage of variance. According to Field (2005), Eigenvalues greater than 1 represent substantial amount of variation in the extracted factors. As it can be noted from Table 4.4, nine factors were responsible for 76.8% of the total variance. Extraction of factors was done at factor loadings greater than 0.5. Factor loadings are correlation coefficients which indicate the relative contribution of each individual variable (or item) on the factor. A substantive importance of a variable to a factor is obtained by squaring the factor loading (Field, 2005).

Factors	Initial Eigenvalues		
	Total	% of Variance	Cumulative %
1	7.257	24.191	24.19
2	3.217	10.724	34.92
3	2.567	8.558	43.47
4	2.205	7.351	50.82
5	1.847	6.155	56.98
6	1.786	5.954	62.93
7	1.609	5.364	68.30
8	1.335	4.450	72.75
9	1.217	4.056	76.80

Table 4.1: Factor analysis - Component extraction

The factor analysis results presented in Appendix D show that there were leakages on items q1.5 and q2.4. Item leakage implies that respondents were confused about the items (Cavana et al., 2001). These items needed to be removed from the questionnaire or replaced with more understandable ones. The items were therefore excluded from subsequent statistical analyses. While literature recommends factor loadings greater that 0.3 (Cavana et al., 2001), factors were extracted at loadings greater than 0.5 in order to reduce number of item leakages.

4.2.1.2 Internal consistency

As already discussed in Section 3.3.9.3, items under each extracted factor were assessed for consistency by checking if the items were highly correlated (Sekaran, 2003).

Factor 1: Items q1.1, q1.3, q1.4 and q1.7 loaded on **Factor 1**. A close examination of these items showed that the items related to user participation in ISRM according to Spears and Barki (2010). The loading of these items on **Factor 1** was an indication of the items' reasonable measurement of the latent variable "User Participation in ISRM". This factor was accordingly named as such and was represented as UP_{ISRM}. The high correlations in Table 4.2 show that (1) the items hanged together as a set, (2) the items independently measured the same concept and (3) the respondents attached the same overall meaning to each of the items in each extracted factor.

Correlations			
Items	Q1.1	Q1.3	Q1.4
Q1.3	.562**		
Q1.4	.575**	.523**	
Q1.7	.598**	.565**	.671**

**. Correlation is significant at the 0.01 level (2-tailed).

Table 4.2: Internal consistency for UP_{ISRM}

Table 4.3 outlines questionnaire items which were identified to be reflective of UP_{ISRM}. These items were cross-checked against those that Stoneburner et al. (2002) as well as Spears and Barki (2010) suggest are in the scope of user participation in ISRM.

UP_{ISRM} roles identified in this study	(Spears & Barki, 2010; Stoneburner et al., 2002)
• Documenting business processes or transactions for risk evaluation (q1.1) • Defining procedural controls such as rules for access control (q1.3) • Implementing controls (q1.4) • Communicating information security regulatory initiatives (q1.7)	• Business process workflow • Risk-control identification • Control design • Control implementation • Control testing • Control remediation • Communication

Table 4.3: Comparison of UP_{ISRM} roles

As it can be noted from Table 4.3, the items underlying UP_{ISRM} were found to be consistent with those that Spears and Barki (2010) and Stoneburner et al (2002) suggested are in the domain of ISRM.

Factor 2: Questionnaire items q3.4, q7.1, q7.2, q7.3, and q8 loaded on **Factor 2**. Referring to the survey instrument presented in Appendix B, these items were reflective of improvement in information security control performance (Stoneburner et al., 2002; Spears & Barki, 2010). **Factor 2** was, therefore, labelled "*improvement in information security control performance*" and represented as IM_{ISCP}. The items were also checked for internal consistency

and results as outlined in Table 4.4 show that the items hanged together as a set, they independently measured the IM_{ISCP} and that the respondents attached the same overall meaning to each of the items. Factors which reflect IM_{ISCP} include reduction in the number or significance of control errors and increase in efficiency across the system of controls in the protection of information from related risks (Spears & Barki, 2010).

Correlations

Items	Q3.4	Q7.1	Q7.2	Q7.3
Q7.1	-.446**			
Q7.2	-.313*	.772**		
Q7.3	-.445**	.608**	.625**	
Q8	-.471**	.512**	.516**	.446**

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Table 4.4: Internal consistency for IM_{ISCP}

Factor 3: Questionnaire items which had loadings on **Factor 3** were q2.1, q2.2, q2.3, and q2.6. Item q2.4 was removed due to its leakage to Factor 8. An examination of these items showed that the items were related to user participation roles in the daily information security control. **Factor 3** was therefore named "*user participation in information security control*" and represented as UP_{ISC}. The items underlying **Factor 3** were also assessed for internal consistency. The high correlations as can be noted in Table 4.5 showed that the items were internally consistent.

Correlations

Items	Q2.1	Q2.2	Q2.3
Q2.2	.535**		
Q2.3	.360*	.553**	
Q2.6	.342*	.380*	.399**

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Table 4.5: Internal consistency for UP_{ISC}

The second area of user participation in ISRM practices, according to Spears and Barki (2010) is information security control. Items which loaded on **Factor 3** were also established to be consistent with those that Spears and Barki (2010) suggest are in the scope of UP_{ISC}. These have been outlined in Table 4.6.

UP_{ISC} roles identifies in this study	UP_{ISC} roles by Spears and Barki (2010)
• Granting access to information resources (q2.1) • Separation (segregation) of duties (q2.2) • Definition of alerts, triggers and application controls (q2.3) • Determining risk tolerance (risk acceptance level) (q2.6)	• Access control • Segregation of duties • Alerts and triggers • Exception reports • End-user computing • Training • Risk tolerance

Table 4.6: Comparison of UP_{ISC} roles

Factor 4: Items with loadings on factor 4 were q1.2, q1.6, q3.1, and q3.3. These items relate to users being held accountable and responsible for ISRM practices. **Factor 4** was therefore labelled "*User accountability and responsibility*" and was represented as $US_{ACC/RESP}$. High correlations as outlined in Table 4.7 show that the items were internally consistent hence hanged together as a set, independently measured user accountability, and responsibility and the respondents attached the same overall meaning to each of the items (Sekaran, 2003).

Correlations

Items	Q1.2	Q1.6	Q3.1
Q1.6	.415**		
Q3.1	.321*	.303*	
Q3.3	.443**	.446**	.623**

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Table 4.7: Internal consistency for $US_{ACC/RESP}$

Factor 5: Questionnaire items which loaded on **Factor 5** were q3.6, q6.1, q6.2, and q6.3. These items relate to information security control development and remediation. **Factor 5** was therefore named as "*user participation in control development*" and was assigned the code UP_{CD}. The high correlations as can be noted in Table 4.8 signify internal consistencies among the items.

Correlations

Items	Q3.6	Q6.1	Q6.2
Q6.1	.299*		
Q6.2	.526**	.536**	
Q6.3	.263	.340*	.556**

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

Table 4.8: Internal consistency for UP_{CD}

There were two items which loaded on **Factor 6** and these were q4 and q5. Following the removal of item q2.4 which had leakage, **Factor 8** had one item

(q3.2). Also item q9 loaded on **Factor 9**. Factor loadings with items less than three are considered to be unstable (Costello & Osborne, 2005). However, unstable factors can still be maintained if they are suitably defined by the underlying items (Hatcher, 1994).

Items q4 and q5 which loaded on **Factor 6** relate to user awareness and sense of ownership for information security practices. This factor was accordingly named "*user demonstrated sense of ownership and awareness*" and given a variable code UD_{SOA}. Items q2.5 and q3.5, which loaded on **Factor 7** relates to user participation in *information security awareness campaigns*. This factor was therefore named as such and given the variable name UP_{ISAC}. **Factor 8** resulted in having item q3.2 which relates to users taking up responsibilities for information security practices. This relates to **Factor 4**. Similarly, **Factor 9** which only had one item loaded relates to **Factor 2**. Based on Hatcher (2003), factors 6 and 7 were maintained.

4.2.2 Reliability analysis

As discussed in Section 3.3.9.4, reliability of the extracted factors was assessed using Cronbach's alpha. Table 4.9 presents a summary of the reliability analysis results. While lower values of α indicate an unreliable scale, values of .7 and even below .7 can be realistic when dealing with psychological constructs (Cavana et al., 2001; Kline, 2000; Sekaran, 2003). This study dealt with constructs which were precisely psychological. Also as discussed in Section 3.3.9.4, the value of α depends on the number of items on the measurement scale. The top half of the α equation includes number of items squared. It is therefore possible to get a large value of α by simply increasing the number of items (Field, 2005).

Factor	Items	Means	Std. Dev.	Alpha
1	4	1.307	0.045	0.845
2	5	3.209	0.274	0.669
3	4	1.313	0.040	0.734
4	4	1.313	0.059	0.731
5	4	1.375	0.102	0.729
6	2	3.102	1.506	0.795
7	2	1.295	0.061	0.617

Table 4.9: Constructs reliability analysis

Results in Table 4.9 show that the numbers of items on the extracted factors were relatively small. These, however, yielded considerably large values of $\propto > .6$. It may therefore be concluded that the large values of α were an indication of the items being reliable.

4.2.3 Descriptive statistics

As discussed in Section 3.3.9.1, the mean and standard deviation were used to assess the centrality and dispersion (spread) of the data. Measures of central tendency and dispersion were obtained for all the items underlying each factor (linear component). The measures were done simultaneously for South Africa and Malawi to establish whether respondents in the two countries understood and reacted to the questionnaire items in the same manner (Sekaran, 2003).

a) Central tendency and dispersion of UP_{ISRM}

Table 4.10 shows means and standard deviations for items underlying UP_{ISRM}. The items were measured on a scale on 1 to 3. As it can be noted, the item means were clustered around 1 reflecting that respondents from the two countries responded "Yes" to users participating in the ISRM roles.

	Malawi		South Africa	
User participation roles in ISRM	**Mean**	**Std. Dev.**	**Mean**	**Std. Dev.**
Q1.1. Documenting business processes or transactions for risk evaluation	1.30	.470	1.24	.436
Q1.3. Defining procedural controls e.g. rules for access control	1.39	.499	1.38	.498
Q1.4. Implementing controls	1.26	.449	1.14	.359
Q1.7. Communicating information security regulatory initiatives	1.30	.470	1.43	.507

Table 4.10: Central tendency and dispersion of UP_{ISRM}

The results in Table 4.10 also show that there is no significant difference between the responses from participants in South Africa and those in Malawi. It may therefore be concluded that users in both countries participate in ISRM practices as those listed in Table 4.10 in the same way.

b) Central tendency and dispersion of IM_{ISCP}

Items underlying IM_{ISCP} were also assessed for their central tendency and dispersion using item means and standard deviation. Results of this assessment are presented in Table 4.11. All the items were measured on a scale of 1 to 5 representing "much worse", "worse", "no change", "better", and "much better" except item q3.4 which was measured on a scale of 1 to 3.

Items underlying IM_{ISCP}	Malawi		South Africa	
	Mean	Std. Dev.	Mean	Std. Dev.
Q3.4. Reviews of Information Security Policy	1.30	.470	1.24	.436
Q7.1. Access control for system users	3.83	.887	3.67	.730
Q7.2. Segregation of duties for system users	3.78	.795	3.62	.669
Q7.3. Information Security Policy	3.91	.733	3.90	.889
Q8. Decreased number of control deficiencies for key controls has decreased	3.39	.839	3.43	.676

Table 4.11: Central tendency and dispersion of IM_{ISCP}

The results show a slight improvement in items q7.1, q7.2, and q7.3 as the item means are generally clustered around 4 which represented "better" on the Likert scale. There was, however, no improvement in item q8 as evidenced by the means clustered around 3 (no change). This was true for both South Africa and Malawi.

c) Central tendency and dispersion of UP_{ISC}

Measures of central tendency and dispersion for items underlying UP_{ISC}, as presented in Table 4.12, show that users in South Africa and Malawi similarly participate in information security controls. This is with an exception of item q2.6 whose the mean for South Africa is 1.57 which is close to 2 i.e. "No" on the Likert scale. This seems to be significantly different from the mean of the same item 1.48 for Malawi.

Items underlying UP_{ISC}	Malawi		South Africa	
	Mean	Std. Dev.	Mean	Std. Dev.
Q2.1. Granting access to information resources	1.30	.470	1.19	.402
Q2.2. Separation (segregation) of duties	1.09	.288	1.19	.402
Q2.3. Definition of alerts, triggers, or application controls	1.35	.487	1.33	.483
Q2.6. Determining risk tolerance (risk acceptance level)	1.48	.511	1.57	.507

Table 4.12: Central tendency and dispersion of UP_{ISC}

d) Central tendency and dispersion of $US_{ACC/RESP}$

Items underlying $US_{ACC/RESP}$ were also assessed for central tendency and dispersion. The items were measured on a scale of 1 to 3 and results in Table 4.13 show that users in South Africa and Malawi are similarly accountable and responsible for ISRM practices.

Items underlying $US_{ACC/RESP}$	Malawi		South Africa	
	Mean	Std. Dev.	Mean	Std. Dev.
Q1.2. Ensuring key controls exist to mitigate specific types of risks	1.22	.518	1.38	.669
Q1.6. Remediating defective controls	1.48	.593	1.19	.402
Q3.1. Individual roles and responsibilities defined and documented	1.39	.499	1.24	.436
Q3.3. Users (data or process owners) made responsible for specific controls	1.35	.573	1.29	.463

Table 4.13: Locality and dispersion of $US_{ACC/RESP}$

e) Central tendency and dispersion of UP_{CD}

Table 4.14 presents means and standard deviations for items underlying UP_{CD}. The items were assessed on a scale of 1 to 3 and the results show that organisational management in South Africa and Malawi similarly support the development of information security controls. However, then means for item q6.1 show a significant difference in the way users participate in control development between South Africa and Malawi. Contrary to the users in South Africa, users in Malawi were reported to participate less in control development by providing information required by control developers as evidenced by the mean 1.57 which is close to 2 (No) on the Likert scale.

As it can also be noted from Table 4.14, respondents in the South Africa and Malawi were similarly reported not to participate in the assessment of information security controls to identify those controls which need remediation. This is signified by means 1.52 and 1.62 which are both close to 2 (no) for Malawi and South Africa respectively.

Items underlying UP_{CD}	Malawi		South Africa	
	Mean	Std. Dev.	Mean	Std. Dev.
Q3.6. Management support demonstrated for Information Security	1.17	.388	1.14	.478
Q6.1. Provide information needed by control designers	1.57	.728	1.38	.590
Q6.2. Documentation of criteria for granting access to information systems	1.30	.559	1.29	.463
Q6.3. Assessment of controls to identify those which need remediation	1.52	.593	1.62	.669

Table 4.14: Central tendency and dispersion of UP_{CD}

f) Central tendency and dispersion of UD_{SOA}

The central tendency and dispersion for items underlying UD_{SOA} were measured on a scale of 1 to 5. The means, as reflected in Table 4.15, which

were close to 3 implied respondents' neutrality on the users' awareness of information security policies as well as users' sense of ownership for protecting information integrity.

Items underlying UD_{SOA}	Malawi		South Africa	
	Mean	Std. Dev.	Mean	Std. Dev
Q4. Users' increased awareness of policies, procedures and the need for information security	2.91	1.20	3.14	1.06
Q5. users demonstrated sense of ownership toward protecting the information integrity	3.35	1.07	3.00	1.10

Table 4.15: Central tendency and dispersion of UD_{SOA}

g) Locality and dispersion of UP_{ISAC}

Items underlying UP_{ISAC} were measured on a scale of 1 to 3. The means and standard deviations for the two items underlying UP_{ISAC} are presented in Table 4.16.

Items underlying UD_{ISAC}	Malawi		South Africa	
	Mean	Std. Dev.	Mean	Std. Dev
Q2.5. Participating in information security awareness campaigns	1.57	0.590	1.24	0.436
Q3.5. Information security policy communicated to users and stakeholders	1.22	0.518	1.14	0.359

Table 4.16: Central tendency and dispersion for UP_{ISAC}

The mean for item q2.5 was close to 2 for responses obtained in Malawi indicating that users in Malawi do not participate in information security awareness campaigns to the same degree as users in South Africa. The mean for item q2.5 in South Africa was close to 1 reflecting user participation in information security awareness campaigns. Means for item q3.5 were both close to 1 implying that information security policies are communicated to all the users and stake holders in the two countries.

4.3 Qualitative methods

The qualitative methods were used to confirm themes and concepts about user participation in ISRM generated from the quantitative data.

4.3.1 User participation roles

Survey participants were asked to provide a list of activities which users in their organisations performed in the past one year, from the time of data collection, as part of ISRM activities. The aim was to solicit ideas and assess the level of knowledge of the survey participants on ISRM activities. Participants were also asked to list activities which are within the scope of ISRM.

These themes were compared with those which were generated through content analysis of the qualitative data. Each theme was checked as to how many times it appeared. This generated a frequency table of themes out of which a chart presented in Figure 4.4 was constructed. These user participation roles in ISRM were established to be consistent with those suggested in literature (Stoneburner et al., 2002; Spears & Barki, 2010).

Results in Figure 4.5 show that development, implementation and remediation of information security controls were listed by 31.7% of the respondents in South Africa as ISRM roles that user performed in the past one year from the time of conducting this research. This was followed by IT risk identification and mitigation (14.6%), testing of new processes, procedures and information security controls (12.2%), and information security awareness campaigns (12.2%). On the contrary, 32.3% of the survey participants in Malawi listed user participation in information security awareness campaigns followed by physical access control to information resources (12.9%) and testing of new process, procedures and information security controls (9.7%).

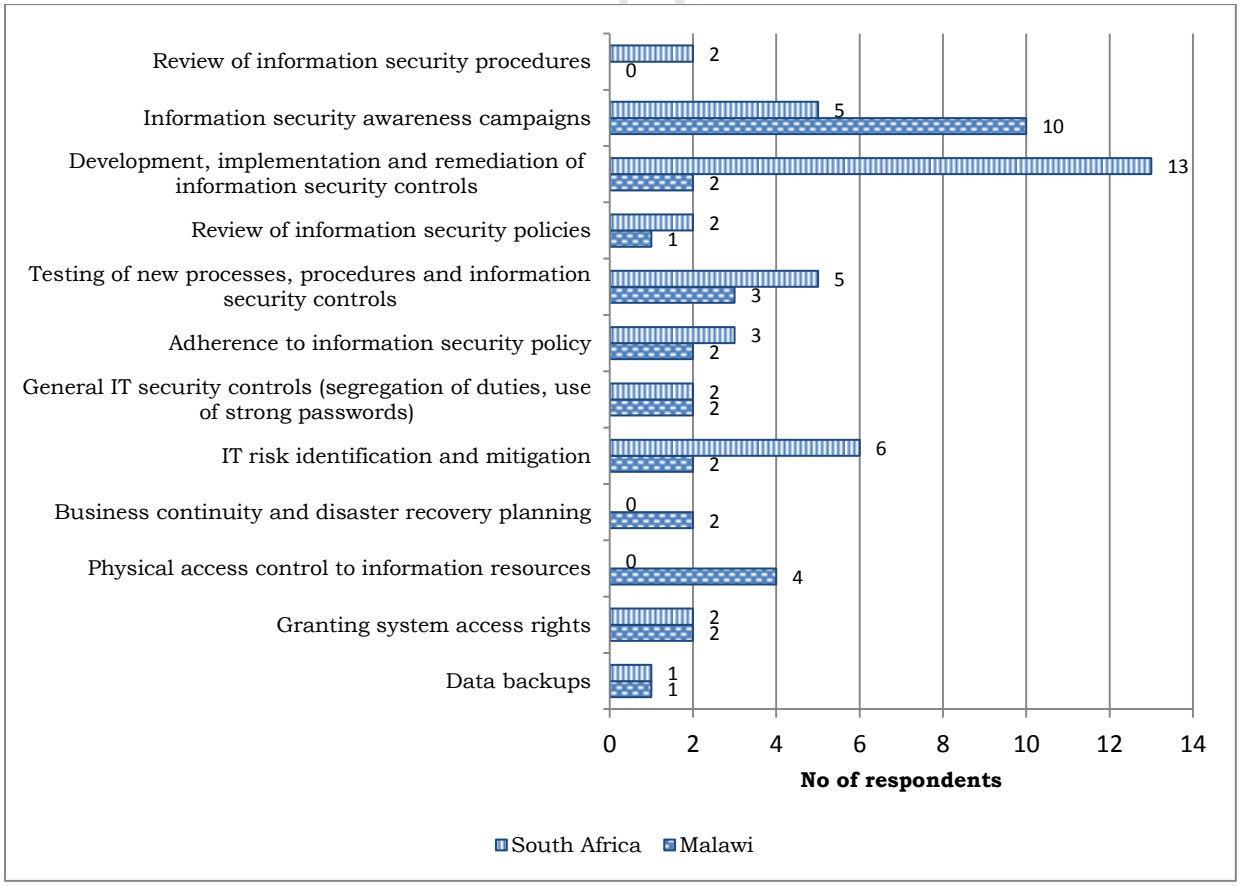

Figure 4.5: User participation roles in South Africa and Malawi

Data collected from the semi-structured interviews also confirmed the user participation roles outlined in Figure 4.5. Further to confirming these results, one interview respondent indicated that granting of access to the billing system at BWB depended on the users. "*User system access details come from the users who exactly know who access what based on the users' lines of duty*". According to the respondent, this information is passed on to the IT department which eventually grants access rights to a particular user based on the system access requirements received from the user's department.

It was also established in a separate interview at BWB that Zone Managers are important when it comes to granting access to the water billing system. "*…when I receive a new member of staff, I am only given the title of the individual by the human resources department. Based on what I already know about that role, I complete a systems access request form which I send to the IT Department for them to create and grant system access to the new member of staff based on details on the form",* reported one Zone Manager. It was also learnt that sometimes the IT Department implements information security controls without prior communication to the user departments.

"*… the problem we usually experience is that our IT Department often makes changes or implements new controls without informing us or without firstly soliciting our views. Just two days ago, the IT Department installed some software on all the computers which has blocked use of flash disks. The problem with that is that our network is often times down due to the frequent power black-outs that we are currently experiencing in this country. Right now, I am stranded; I can't print anything simply because we only have one network printer at this zone. I have the report on my computer but I can no longer use my flash disk to get it printed at another zone office",* also noted one Zone Manager.

This concern of lack of prior communication was also shared by another Zone Manager and the Planning and Development Manager. In addition, it was also established that no systems audits were conducted at BWB up until the time of conducting this study.

"… BWB only depends on external audits when it comes to systems audits which I think is a big problem because those audits are only scheduled once a year. I know the importance of continuously monitoring user activities in the billing system. It is

necessary that we also perform systems audits and not to wait until the scheduled external audits" reported one interview participant.

4.3.2 Information security awareness

While user participation in information security awareness campaigns was the second highly listed user participation role in South Africa, this was not one of the user participation roles in ISRM that participants in Malawi listed. Instead, the second highly listed user participation role in Malawi was general IT security controls, which includes segregation of duties, use of strong passwords, not sharing passwords and many more. This signifies the difference in the way users in South Africa and Malawi participate in ISRM practices. User awareness about information security is endorsed in literature (David, 2002; Doherty & Fulford, 2005; Siponen, 2000a) as an important element of ISRM. Despite user participation in information security awareness campaigns not being listed by the survey participants in Malawi, it came up in one of the interviews at BWB. The interview respondent noted that:

"*…users play a very important role in disseminating information about changes in the information security policy amongst fellow users. We have not usually conducted organisation-wide awareness campaigns when we effect some changes or implement new controls. Instead, we always make sure that a few users get to know the changes then the information is passed on to their fellow users and eventually the whole BWB become aware of the changes.*"

4.3.3 Physical access control and business continuity planning

Survey participants in Malawi also listed physical access control to information resources as well as business continuity and disaster recovery planning as activities that users participated in the past one year from the time this study was conducted. However, survey participants in South Africa did not list these roles as having been performed by users in the past one year from the time this study was conducted. This further outlines the difference between Malawi and South Africa on how users participate in ISRM.

4.4 Testing of hypothesis

Researchers in scientific research are usually interested in finding relationships between variables or constructs (Field, 2005). A hypothesis is a prediction that some kind of effect or relationship exists between the concepts being studied.

Hypothesis testing aims at explaining the nature of relationships among groups of factors (Cavana et al., 2001; Sekaran, 2003).

As already outlined in Section 3.3.2, the type of investigation adopted in this study was correlational. In a correlational investigation, predictions (hypotheses) are checked whether they hold or not by observing the associations amongst the items underlying the variables of interest (Cavana et al., 2001). For instance, to check whether user participation contributes to information security management, associations through correlation coefficients of items underlying user participation and those items underlying information security management were checked for significance.

H1. User participation in ISRM contributes to effective information security management

To test the above hypothesis, associations of items underlying user participation and those reflective of improvement in information security control performance IM_{ISCP} were checked. Literature proposes three areas in users participate as part of information security management. The areas include user participation in the ISRM processes, user participation in Information Security Control (ISC), and user participation through accountability roles (ACC) (Spears & Barki, 2010).

a) Association between user participation in ISRM and improvement in ISCP

The items which were used to measure user participation in ISRM included item q1.1, q1.3, q1.4, and q1.7 while items which measured user participation in ISC included item q3.4, q7.1, q7.2, q7.3 and q8. As it can be noted from Table 4.17, items which measured user participation in ISRM were reasonably correlated.

	Items underlying improvement in ISCP				
Items underlying user participation in ISRM	Q3.4	Q7.1	Q7.2	Q7.3	Q8
Q1.1. Documenting business processes or transactions for risk evaluation	.427**	-.127	-.243	-.316*	-.130
Q1.3. Defining procedural controls for example rules for access control	.038	.015	-.063	-.203	.003
Q1.4. Implementing controls	.196	-.053	-.104	-.368*	.024
Q1.7. Communicating Information Security regulatory initiatives	.174	.059	-.083	-.271	.092

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Table 4.17: Correlation of user participation in ISRM and improvement in ISCP

Also worth noting are the significant associations between the paired items q1.1:q3.4, q1.1 and q7.3, and q1.4:q7.3. With the correlational investigation type which was employed in this study, the results in Table 4.17 substantiate the conclusion that user participation in ISRM contributes to improvement in ISCP. These results were consistent with literature (Chang & Ho, 2006; Siponen, 2005; Spears & Barki, 2010; Stanton & Stam, 2006; Whitman, 2008), which posit that user participation in ISRM contributes to improvement in control performance.

b) Association between user participation in ISC and improvement in ISCP

Correlational associations between items which measured user participation in ISC and those which measured improvement in ISCP were also assessed. Results as presented in Table 4.18 show that these two constructs were reasonably correlated. Also worth noting are the significant associations between q2.3 and q7.2 as well as items 2.6 and q7.3.

	Items underlying improvement in ISCP				
Items underlying user participation in ISC	Q3.4	Q7.1	Q7.2	Q7.3	Q8
Q2.1. Granting access to information resources	.236	-.147	-.127	-.265	.035
Q2.2. Separation (segregation) of duties	-.095	.124	-.021	-.122	.048
Q2.3. Definition of alerts, triggers, or application controls	.098	-.135	-.368*	-.220	-.009
Q2.6. Determining risk tolerance (risk acceptance level)	.279	-.185	-.264	-.397**	.036

**. Correlation is significant at the 0.01 level (2-tailed).
*. Correlation is significant at the 0.05 level (2-tailed).

Table 4.18: Correlation of user participation in ISC and improvement in ISCP

The results in Table 4.18 also were in support of the literature which posits that user participation in ISRM practices contributes to the efficient management of information security (Chang & Ho, 2006; Siponen, 2005; Spears & Barki, 2010; Stanton & Stam, 2006; Whitman, 2008).

c) Association between user participation in ACC/RESP and improvement in ISCP

The results in Table 4.19 are also consistent with literature (Chang & Ho, 2006; Siponen, 2005; Spears & Barki, 2010; Stanton & Stam, 2006; Whitman, 2008) which posits that user participation in ISRM practices contributes to the efficient management of information security.

	Items underlying improvement in ISCP				
Items underlying user participation in ACC/RESP	Q3.4	Q7.1	Q7.2	Q7.3	Q8
Q1.2. Ensuring key controls exist to mitigate specific types of risks	.213	-.278	-.275	-.284	.035
Q1.6. Remediating defective controls	.089	-.123	-.215	-.366*	-.125
Q3.1. Individual roles and responsibilities defined and documented	.349*	-.274	-.193	-.291	-.047
Q3.3. Users (data or process owners) made responsible for specific controls	.317*	-.305*	-.359*	-.433**	-.162

**. Correlation is significant at the 0.01 level (2-tailed).
*. Correlation is significant at the 0.05 level (2-tailed).

Table 4.19: User participation in ACC/RESP and improvement in ISCP

All the results in Table 4.18, Table 4.19 and Table 4.20 show that user participation in ISRM practices contributes to the efficient management of information security. This resulted in hypothesis **"H1"** that user participation in ISRM contributes to the efficient management of information security being accepted.

The second objective of this study was to understand how different national cultures influence user participation in ISRM which may impact the management of information security. These results support the body of literature which posits that user participation contributes to the efficient management of information security (Chang & Ho, 2006; Siponen, 2005; Spears & Barki, 2010; Stanton & Stam, 2006; Whitman, 2008).

H2. User participation in ISRM practices is the same in South Africa and Malawi

To test for the validity of this hypothesis, means for items underlying the various constructs were assessed for significant differences through the parametric *t*-test as discussed in Section 3.3.9.5.

a) Difference between means for user participation in ACC/RSEP

As it can be noted from Table 4.20, there were non-significant p-values for all the items except item Q1.6 (Remediating defective controls). Firstly, the equal variance assumption was violated for this item. Levene's test for variance homogeneity shows a significant p-value of .001. The second row of results (Equal variances not assumed) shows a 2-tailed significant p-value of .044. Tested at significance level of .05, this indicates that the difference between

the means of this item for the two countries was significant. An examination of the means for item q1.6 showed that users in Malawi do not participate to the same degree as their counterparts in South Africa. With mean = 1.50 and Std. Error = 1.20 for Malawi and mean = 1.19 and Std. Error = 0.088 for South Africa, the difference between the means was significant at $t(43) = 2.026, p < .05$.

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Q1.2. Ensuring key controls exist to mitigate specific types of risks	Equal variances assumed	1.938	.171	-.731	43	.469	-.131	.179	-.492	.230
	Equal variances not assumed			-.720	38.092	.476	-.131	.182	-.499	.237
Q1.6. Remediating defective controls	Equal variances assumed	11.917	.001	2.026	43	.049	.310	.153	.001	.618
	Equal variances not assumed			2.077	40.726	.044	.310	.149	.009	.611
Q3.1. Individual roles and responsibilities defined and documented	Equal variances assumed	3.870	.056	.978	43	.333	.137	.140	-.145	.419
	Equal variances not assumed			.986	42.994	.329	.137	.139	-.143	.417
Q3.3. Users (data or process owners) made responsible for specific controls	Equal variances assumed	1.684	.201	.568	43	.573	.089	.157	-.228	.406
	Equal variances not assumed			.576	42.722	.568	.089	.155	-.223	.402

Table 4.20: Differences between means for user participation in ACC/RESP

b) Difference between means for user participation in ISAC

Means for items (q2.5 and q3.5) underlying user participation in ISAC were also tested for significant differences between the data collected in South Africa and that from Malawi. Results in Table 4.21 show that the variance homogeneity assumption was invalidated by the non-significant F-value of 1.152 at a p-value of .289 for item q3.5. The corresponding $t(43) = 0.492$ was also found to be non-significant at $p > .05$. The Levene's test for equal variances for item q2.5 (Participating in information security awareness campaigns) validated the variance homogeneity assumption. As it can be noted from Table 4.21, the *t*-test results for item q2.5 under the "equal variance not assumed" row showed a significant difference between the item means with $t(43) = 2.264, p = .029$. An examination of the means for item q2.5 showed that users in South Africa participated more with $Mean = 1.58$ and $Std. Error\ Mean = .119$ than users in Malawi with $Mean = 1.24$ and $Std. Error\ Mean = .095$

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Q2.5	Equal variances assumed	7.059	.011	2.220	43	.032	.345	.155	.032	.659
	Equal variances not assumed			2.264	42.045	.029	.345	.153	.037	.653
Q3.5	Equal variances assumed	1.152	.289	.492	43	.625	.065	.133	-.203	.334
	Equal variances not assumed			.503	41.235	.617	.065	.130	-.197	.328

Table 4.21: Means for items underlying user participation in ISAC

These results were not in support hypothesis **H2** which posits that participation of users in ISRM in South Africa is the same as that of users in Malawi dependent on national cultures. The differences in user behaviour as influenced by culture are reflected in the outcomes of the users' participation in ISRM. Therefore, one country's success in information security management as a result of user participation in ISRM would not imply another country's success.

4.5 Chapter summary

This chapter presents the results from data analysis as well as the discussions for the findings. First, the chapter presents the demographic characteristics of the study participants. These are based on educational and professional qualifications as well as the industrial types. Second, the chapter outlines quantitative data analysis results which are structured in four sub sections: locality and dispersion, distribution, goodness of the data and reliability checks. Third, the chapter provides the qualitative data analysis results. The forth section presents results for the hypothetical tests which were conducted in order to check or validate the claims discovered in literature. Lastly, the findings of the study are discussed.

Chapter 5 : Conclusion and Recommendations

This chapter summarizes the study by identifying the research methods used in the study. It also discusses the research findings as well as the implications of the study.

5.1 Introduction

This study was based on two problem areas. Firstly, there are contradicting views about how user participation in ISRM contributes to the management of information security. Users are portrayed as a weak links to information security (Dojkovski et al., 2011; Lim et al., 2009; Siponen & Oinas-Kukkonen, 2007; Steele & Wargo, 2007; Thomson et al., 2006) or as a solution to some of the information security problems (Chang & Ho, 2006; Siponen, 2005; Spears & Barki, 2010; Stanton & Stam, 2006; Whitman, 2008). Based on these contradictions, the first objective of this study was to understand how user participation in ISRM contributes to information security management.

Literature suggests that culture influences user attitude and behaviour towards ISRM practices (Chow et al., 1994). However, studies which focus on understanding how different cultures influence user participation in ISRM practices are rare (Chang & Ho, 2006; Dinev & Hu, 2007; Spears & Barki, 2010). This study was also aimed at understanding how user participation in ISRM practices varies across nations of different national cultures.

The study was guided by two research questions. Firstly, the researcher was interested in understanding how user participation in ISRM contributes to the efficient management of information security. Secondly, the researcher wanted to understand how national cultures influence user participation in ISRM practices which may have an impact on the management of information security.

A mixed methods approach was employed in this study to collect, analyse and interpret data. The results acquired from qualitative methods were used to elaborate (complement) and to confirm (triangulate) those results acquired from the quantitative methods (Migiro & Magangi, 2011).

5.2 Summary of the findings

F1. The findings in this study showed that user participation in ISRM practices contributes to the effective management of information security.

F2. Secondly, the findings of the study revealed that participation of users in ISRM practices is different between South Africa and Malawi.

F3. The findings of this study also showed that government and financial institutions have healthy appetites for information security management as compared to other industries.

5.2.1 User participation in ISRM

Spears and Barki (2010) suggest three areas of user participation in ISRM practices: user participation in ISRM, user participation in information security control, and user participation through accountability roles. Reflective items for each of these constructs were confirmed to have correlational links with improvement in information security control performance. This was found to be consistent with the literature which posts that user participation in ISRM contributes to the efficient management of information security (Chang & Ho, 2006; Siponen, 2005; Spears & Barki, 2010; Stanton & Stam, 2006; Whitman, 2008).

5.2.2 Cultural influence on user participation in ISRM practices

The comparison of the questionnaire item means for the data collected in South Africa and Malawi showed that there was significant difference between user participation in remediating defective controls for the two countries. While the t-test results revealed the significance of this difference, an examination of the means for this item showed that users in Malawi do not participate in remediating defective controls to the same degree as users in South Africa do.

Secondly, the t-test results also revealed a significant difference between user participation in information security awareness campaigns for the two countries. A comparison of means for user participation in information security awareness campaigns revealed that users in South Africa do not participate in information security awareness campaigns to the same degree as users in Malawi do.

These differences in user participation roles in ISRM were attributed to differences in national cultures. This was based on Harrison (1992) and Chow et al. (1994) who posit that culture influences user behaviour towards management practices.

5.2.3 Information security management appetites

The findings of the study further suggest healthy appetites for information security management demonstrated by government departments and financial institutions

in the two countries. The healthy appetites were reflected by relatively large numbers of information security administrators and information systems auditors working in these industries as compared to other industries.

5.3 Implications of the study

5.3.1 Academic community

Academic scholars with an appetite for global information security management would find this study as necessary. Research studies with particular focus on integrated information security management may be guided by the findings in this study as they outline the importance of national cultures in the way users behave towards ISRM practices. This study was one response to the recent calls for further examination of causal factors which influence behaviours in social networks within different cultures, race and ethnic groups (De Souza & Dick, 2009; Ellison, Steinfield, & Lampe, 2007; Yum & Hara, 2006). The findings of this study can therefore be used when planning and executing future research in the same research domain.

5.3.2 Governments

There are insignificant deterrent effects on domestic enforcement against cyber-attacks (Pang et al., 2010). Interdependent information security management efforts allow governments to directly address information security through enforcement against cyber-attacks (Wang & Kim, 2009). It is therefore important for one country to understand how users in other countries perceive and respond to ISRM initiatives in order to have coordinated information security management efforts. This study provides knowledge on how users in South Africa and Malawi participate in ISRM. Information security management efforts involving the two countries would therefore use the findings of this study to draft and implement information security policy which would ensure policy harmonization.

5.3.3 Practitioners

Organisations also need to understand how national cultures influence people's attitude and behaviour in countries that they conduct business with. This study highlights the differences in user participation in ISRM between users in South Africa and those in Malawi. While users in Malawi were found to participate more in information security awareness campaigns, users in South Africa participate more in remediating defective information security controls. Organisations

operating in these two countries would find the findings of this study necessary as they highlight user behavioural patterns as influenced by cultures in the two countries. This study would also be useful for IT companies that deploy global IT solutions as the successful implementations of the IT solutions largely depend on the users' perceived ease of use of the IT solution.

5.4 Weaknesses and limitations

The low response rate to the survey questionnaire in the context of South Africa may have impacted the findings. The lack of local chapter in Malawi where participants to the study would have been selected from probabilistically so as to enable inference the study findings to a larger population also affected the quality and dependability of the study findings. However, considering the educational as well as professional profiles of the participants to the study, the findings of this study would arguably be of value to the academic community, government departments and transnational organisations.

5.5 Considerations for future research

This study calls for more research studies which would visibly explain the causal factors which influence user behaviours towards ISRM practices within different cultures, race and ethnic groups. While cultural influence on user participation and how this contributes to information security management was one of the objectives of this study, the other observable characteristics of culture also need to be understood. This study calls for more research which would explain how user awareness, responsibility, motivation and commitment over ISRM practices are influenced by different cultures and how these contribute to the management of information security. If conducted at regional level such as SADC, the studies can create good grounds for achieving globalisation in the management of information security.

5.6 Thesis summary

This thesis has reported the importance of understanding how national cultures influence user participation in ISRM which, in turn, contributes to the efficient management of information security. The study was in context of South Africa and Malawi. The study highlighted the importance for the academic community, governments and transnational organisations to understand how national cultures influence user attitude and behaviour towards ISRM practices.

Chapter 6 : References

Adams, A., Templeton, G., & Campbell, N. (2007). *A meta-analysis of security risk theory literature in IS from 2000-2006.* Paper presented at the 2007 American Conference on Information Systems (AMCIS). Retrieved August 12, 2012 from http://aisel.aisnet.org/amcis2007/230

Akers, R. L., & Sellers, C. S. (1994). *Criminological theories: Introduction, evaluation, and application*. Los Angeles, CA: Roxbury Publishing.

Alberts, C. J., & Dorofee, A. J. (2003). *Managing information security risks: The OCTAVE approach.* Upper Saddle River, NJ: Addison-Wesley Professional.

Anderson, R., & Moore, T. (2006). The economics of information security. *Science, 314*(5799), 610-613.

Applegate, L. M., McFarlan, F. W., & McKenney, J. L. (1999). *Corporate Information Systems Management: Text and Cases* (5th ed.). Chicago: Irwin.

Asai, T., Siripukdee, S., Waluyan, L., & Noguera, S. (2009). Potential problems on information security management in cross-cultural environment – A study of cases of foreign companies including Japanese companies in Thailand. *International Journal of Japan Association for Management Systems, 1(1),* 91-100.

Austin, R. D., & Darby, C. A. (2003). The myth of secure computing. *Harvard Business Review, 81*(6), 120-6, 138.

Axelrod, R., & Cohen, M. D. (2000). *Harnessing complexity: Organizational implications of a scientific frontier*. New York: The Free Press.

Bachore, Z., & Zhou, L. (2009). A critical review of the role of user participation in IS success. Paper presented to 2009 AMCIS. Retrieved May 20, 2012 from http://aisel.aisnet.org/amcis2009/659

Barki, H., & Hartwick, J. (1989). Rethinking the concept of user involvement. *MIS Quarterly, 13(1),* 53-63.

Barki, H., & Hartwick, J. (1994). Measuring user participation, user involvement, and user attitude. *Mis Quarterly, 18(1),* 59-82.

Baskerville, R. (1993). Semantic database prototypes. *Information Systems Journal, 3*(2), 119-144.

Biernacki, P., & Waldorf, D. (1981). Snowball sampling: Problems and techniques of chain referral sampling. *Sociological Methods and Research,* (10), 141-163.

Bishop, M. (2003). *Computer security, art and science.* Boston, MA: Addison-Wesley.

Bodin, L. D., Gordon, L. A., & Loeb, M. P. (2008). Information Security and Risk Management. *Communications of the ACM, 51(4),* 64-68.

Brown, I., Hoppe, R., Mugera, P., Newman, P., Stander, A. (2004). The impact of national environment on the adoption of internet banking: Comparing Singapore and South Africa. *Journal of Global Information Management. 12(2),* 1-26.

Burton, F. G., Chen, Y. N., Grover, V., & Stewart, K. A. (1992). An application of expectancy theory for assessing user motivation to utilize an expert system. *Journal of Management Information Systems, 9(3),* 183-198.

Cabrera, A., & Cabrera, E. F. (2002). Knowledge-sharing dilemmas. *Organization Studies, 23(5),* 687-710.

Cavana, R. Y., Delahaye, B. L., & Sekaran, U. (2001). *Applied business research: Qualitative and quantitative methods. (3rd ed.).* Australia: John Wiley

Chang, S. E., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems, 106(3),* 345-361.

Chen, Y., & Zahedi, F.M. (2009, December, 14). *Internet users' security behaviors and trust.* Paper presented at the 2009 Pre-ICIS Workshop on Privacy and Security, Phoenix, Arizona.

Chow, C. W., Kato, Y., & Shields, M. D. (1994). National culture and the preference for management controls: An exploratory study of the firm-labor market interface. *Accounting, Organizations and Society, 19(45),* 381-400.

Chua, W. F. (1986). Radical developments in accounting thought. *Accounting Review, 61(4),* 601-632.

Coleman, J. S. (1958). Relational analysis: The study of social organizations with survey methods. *Human Organization, 17*, 28-36.

Collins, J., & Hussey, R. (2003). *Business research: A practical guide for undergraduate and postgraduate students.* Hampshire: Palgrave Macmillan.

Cook, K. S., & Emerson, R. M. (1978). Power, equity and commitment in exchange networks. *American Sociological Review, 43(5),* 721-738.

Cooper, R. B. (1994). The inertial impact of culture on IT implementation. *Information & Management, 27(1),* 17-31.

Cortina, J. M. (1993). What is coefficient alpha? An examination of theory and applications. *Journal of Applied Psychology, 78(1)*, 98-104.

Costello, A. B., & Osborne, J. W. (2005). Best practices in exploratory factor analysis: Four recommendations for getting the most from your analysis. *Practical Assessment, Research & Evaluation, 10(7)*, 1-9.

Creswell, J. W. (2009). *Research design: Qualitative, quantitative and mixed methods approaches* (3rd ed.). Thousand Oaks, CA: Sage Publications.

Crotty, M. (1998). *The foundations of social research: Meaning and perspective in the research process.* Thousand Oaks, CA: Sage Publications.

Da Veiga, A., & Eloff, J. H. P. (2007). An information security governance framework. *Information Systems Management, 24(4)*, 361-372.

Da Veiga, A., & Eloff, J. H.P. (2010). A framework and assessment instrument for information security culture. *Computers & Security, 29,* 196–207.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20(1),* 79-98.

David, J. (2002). Policy enforcement in the workplace. *Computers & Security, 21*(6), 506-513.

De Campeaux, D. (2002). Taking responsibility for worms and viruses. *Communications of the ACM, 45(4),* 15-16.

Denison, D. R. (1990). *Corporate culture and organizational effectiveness.* New York: Wiley.

De Long, D. W., & Fahey, L. (2000). Diagnosing Cultural Barriers to Knowledge Management. *The Academy of Management Executive, 14(4),* 113-127.

De Souza, Z., & Dick, G. N. (2009). Disclosure of information by children in social networking-not just a case of. *International Journal of Information Management, 29(4),* 255-261.

Dhillon, G., & Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium. *Communications of the ACM, 43(7),* 125-128.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal, 16(3)*, 293-314.

Lumley, T., Diehr, P., Emerson, S. & Chen, L. (2002). The importance of the normality assumption in large public health data sets. *Annual Reviews Public Health, 23*, 151-169.

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems, 8(7)*, 386-408.

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: The role of national culture differences. *Information Systems Journal, 19(4),* 391-412.

Doherty, N. F., & Fulford, H. (2005). Do information security policies reduce the incidence of security breaches: An exploratory analysis. *Information Resources Management Journal, 18(4)*, 21-39.

Doherty, N.F., & Perry, I. (2001). The cultural impact of workflow management systems in the financial services sector. *Service Industries Journal, 21*(4), 147-166.

Dojkovski, S., Lichtenstein, S., & Warren, M. (2011). Fostering information security culture in small and medium size enterprises: An interpretive study in australia. *Proceedings of the 15th European Conference on Information Systems,* 1560-1571.

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of facebook "friends:" Social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication, 12*(4), 1143-1168.

Eloff, M. M., & Von Solms, S. H. (2000). Information security management: An approach to combine process certification and product evaluation. *Computers & Security, 19(8),* 698-709.

Fakun, D., & Greenough, R. M. (2004). An exploratory study into whether to or not to include users in the development of industrial hypermedia applications. *Requirements Engineering, 9(1),* 57-66.

Faugier, J., & Sargeant, M. (1997). Sampling hard to reach populations. *Journal of Advanced Nursing, 26*, 790-797.

Field, A. (Ed.). (2005). *Discovering statistics using SPSS* (2nd Ed.). London: Sage Publication.

Field, A. P. (2009). *Discovering statistics using SPSS* (3rd Ed.). London: SAGE Publications.

Finne, T. (2000). Information systems risk management: Key concepts and business processes. *Computers & Security, 19(3),* 234-242.

Fitzgerald, B., & Howcroft, D. (1998). Towards dissolution of the IS research debate: From polarization to polarity. *Journal of Information Technology, 13*, 313-326.

Fitzgerald, T. (2007). Building management commitment through security councils, or security council critical success factors. In H. F. Tipton (Ed), *information security management handbook.* Hoboken: Auerbach Publications.

Forster, P. G. (1994). Culture, nationalism, and the invention of tradition in malawi. *The Journal of Modern African Studies, 32*(03), 477-497.

Geek, W. (2008). *What is information security?* Retrieved August 23, 2012, from www.wisegeek.com/what-is-information-security.htm

Geertz, C. (1973). *The interpretation of cultures.* New York: Basic Books.

Ghauri, P., & Grønhaug, K. (2002). *Research methods in business studies. A practical guide.* Harlow, Essex: Pearson Education.

Giannoccaro, A., Shanks, G., & Darke, P. (1999). Stakeholder perceptions of data quality in a data warehouse environment. *Australian Computer Journal, 31*(4), 110-116.

Gobbin, R. (1998). The role of cultural fitness in user resistance to information technology tools. *Interacting with Computers, 9(3)*, 275-285.

Goel, S., & Salganik, M. J. (2010). Assessing respondent-driven sampling. *Proceedings of the National Academy of Sciences, 107(15)*, 6743.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2005). CSI/FBI computer crime and security survey. *Computer Security Institute, 25*, 1-25.

Gray, D. (2009). *Doing research in real world*. London: Sage Publications.

Gregor, S. (2002). A theory of theories in information systems. *Information Systems Foundations: Building the Theoretical Base,* 1-20.

Gruber, T. R. (1993). A translation approach to portable ontology specifications. *Knowledge Acquisition, 5*(2), 199-220.

Guba, E. G. (1990). *The paradigm dialog.* Newbury Park, CA: Sage Publications

Guba, E. G., & Lincoln, Y. S. (1988). Do inquiry paradigms imply inquiry methodologies. *Qualitative Approaches to Evaluation in Education,* 89-115.

Guba, E.G and Lincoln, Y, (1994). *Competing paradigms in qualitative research*, In N.K. Denzin, and. Y.S. Lincoln (Eds.), Handbook of Qualitative Research, Thousand Oaks, CA: Sage, 105-117.

Guo, L. (2008). An analysis of 22 years of research in JPIM. *Journal of Product Innovation and Management, 25*, 249-260.

Harris, D., & Davidson, R. (1999). Anxiety and involvement: Cultural dimension of attitudes toward computers in developing societies. *Journal of Global Information Management, 7(1)*, 26-38.

Harrison, G. L. (1992). The cross-cultural generalizability of the relation between participation, budget emphasis and job related attitudes. *Accounting, Organizations and Society, 17(1)*, 1-15.

Hart, S. D. (1998). The role of psychopathy in assessing risk for violence: Conceptual and methodological issues. *Legal and Criminological Psychology, 3(1)*, 121-137.

Hatcher, L. (1994). *A step-by-step approach to using the SAS system for factor analysis and structural equation modeling* SAS Publishing.

He, J., & King, W. R. (2008). The role of user participation in information systems development: Implications from a meta-analysis. *Journal of Management Information Systems, 25(1)*, 301-331.

Hendriks, V. M., Blanken, P., Adriaans, N. F. P., & Hartnoll, R. (1992). *Snowball sampling: A pilot study on cocaine use.* Rotterdam: IVO.

Hinde, S. (2002). Security surveys spring crop. *Computers & Security, 21(4)*, 310-321.

Hirschheim, R., & Klein, H. K. (1992). Conceptual advances. *Advances in Computers, 34*, 293.

Hofstede, G. (2001). *Culture's consequences: Comparing values, behaviors, institutions and organizations across nations (2nd ed.)*. Thousand Oaks, CA: Sage Publications.

Howe, K. R. (1988). Against the quantitative-qualitative incompatibility thesis or dogmas die hard. *Educational Researcher, 17(8)*, 10-16.

Hussey, J., & Hussey, R. (1997). *Business research: A practical guide for undergraduate and postgraduate students.* London: Macmillan.

Im, G.P., & Baskerville, R.L. (2005). A longitudinal study of information system threat categories: The enduring problem of human error. *The Data Base for Advances in Information Systems, 36(4),* 68-79.

Ives, B. & Jarvenpaa, S. L. (1991). Applications of global information technology: Key issues for management. *MIS Quarterly*, *15(1)*, 32-49.

ISACA, C. (2008). Information systems audit and control association: CISA review manual 2008 (2007).

Jahner, S., & Krcmar, H. (2005). Beyond technical aspects of information security: Risk culture as a success factor for IT risk management. Paper presented at the 2005 AMCIS Conference. Retrieved August 10, 2012 from http://aisel.aisnet.org/amcis2005/462

Jarvis, C. B., MacKenzie, S. B., & Podsakoff, P. M. (2003). A critical review of construct indicators and measurement model misspecification in marketing and consumer research. *Journal of Consumer Research, 30(2)*, 199-218.

Jiang, J. J., Klein, G., & Hong-Gee, C. (2006). The effects of user partnering and user non-support on project performance. *Journal of the Association for Information Systems, 7(2)*, 68-88.

Johns, S. K., Murphy Smith, L., & Strand, C. A. (2003). How culture affects the use of information technology. *Accounting Forum, 27(1)*, 84-109.

Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed methods research: A research paradigm whose time has come. *Educational Researcher, 33(7)*, 14-26.

Johnston, A.C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly, 34(3),* 549-566.

Jones, A. (2007). A framework for the management of information security risks. *BT Technology Journal, 25(1)*, 30-36.

Kim, C. S., & Peterson, D. K. (2003). A comparison of the perceived importance of information systems development strategies by developers from the United States and Korea. *Information Resources Management Journal, 16(2)*, 1-18.

Klein, H. K., & Myers, M. D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly, 42(1)*, 67-93.

Kline, P. (2000). *The handbook of psychological testing (2nd ed.).* London; New York : Routledge.

Komatsu, A. (2008). Activities of IPA concerning information security and behavior. In *Lecture Notes of the Symposium on Security Psychology and Trust.* pp. 49-62.

Krauss, S. E. (2005). Research paradigms and meaning making: A primer. *The Qualitative Report, 10(4)*, 758-770.

Kwak, D., Kizzier, D.M., Zo, H., & Jung, E. (2011). Understanding security knowledge and national culture: A comparative investigation between Korea and the U.S. *Asia Pacific Journal of Information Systems, 21(3),* 51-68.

Kyobe, M. (2009). Factors influencing SME compliance with government regulation on use of IT: The case of South Africa. *Journal of Global Information Management (JGIM), 17(2)*, 30-59.

Kyobe, M. (2010). Towards a framework to guide compliance with IS security policies and regulations in a university. *Information Security for South Africa (ISSA), ,* 1-6.

Kyobe, M., Matengu, S., Walter, P., & Shongwe, M. (2012). *Factors influencing recognition and reporting of losses from cyber-attacks: The case of government departments in the Western Cape Province of South Africa.* Paper presented at the 2012 ECIME Conference, Cork, Ireland.

Lee, J., & Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information Management & Computer Security, 10(2)*, 57-63.

Lee, N. J., & Lings, I. (2008). *Doing business research: A guide to theory and practice.* London: Sage.

Leidner, D.E., & Kayworth, T. (2006). A review of culture in information systems research: Toward a theory of information technology culture conflict. *MIS Quarterly, 30(2),* 357-399.

Levy, Y., & Ellis, T. J. (2006). A systems approach to conduct an effective literature review in support of information systems research. *Informing Science, 9,* 181-212.

Lian, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly, 33(1),* 71-90.

Lim, J. S., Chang, S., Maynard, S., & Ahmad, A. (2009). *Exploring the relationship between organizational culture and information security culture.* Paper presented at the 7th Australian Information Security Management Conference. Retrieved May 11, 2012 from http://ro.ecu.edu.au/ism/12

Maitland, C. F., & van Gorp, A. (2009). Beyond harmonization: ICT policymaking in regional economic communities. *The Information Society, 25(1)*, 23-37.

Manda, T. D. (2010). *Maturity of cyber security initiatives in malawi: A comparison with the drive for fast and ubiquitous internet connectivity.* Retrieved August 3, 2012, from http://www.diplomacy.edu/sites/default/files/IGCBP2010_2011_Manda.pdf

Markus, H. R., & Kitayama, S. (1991). Culture and the self: Implications for cognition, emotion, and motivation. *Psychological Review, 98(2)*, 224-253.

Markus, M. L., & Mao, J. Y. (2004). Participation in development and implementation-updating an old, tired concept for today's IS contexts. *Journal of the Association for Information Systems, 5(11)*, 514-544.

Martins A, Eloff, J. (2002, May 7-9). *Information security culture*. Paper presented at the 2002 IFIP TC11 International Conference on information Security, Cairo, Egypt.

McCoy, S., Galletta, D.F., & King, W.R. (2005) Integrating national culture into IS research: The need for current individual level measures. *Communications of the Association for Information Systems. 15,* 211-224.

McGill, T., & Klobas, J. (2008). User developed application success: Sources and effects of involvement. *Behaviour & Information Technology, 27(5)*, 407-422.

McKeen, J. D., & Guimaraes, T. (1997). Successful strategies for user participation in systems development. *Journal of Management Information Systems, 14(2)*, 133-150.

Medina, M., & Caparro, J. (2007). The impact of the human element in the information system quality for decision making and user satisfaction. *Journal of Computer Information Systems, 34(2)*, 21-35.

Meyer, J. P., & Allen, N. (1984). The handbook of employee engagement: Perspectives, issues, research and practice. *Journal of Applied Psychology, 69*, 372-378.

Michalsons, L. (2005). *Guide to the ECT act.* Retrieved November, 18, 2012 from http://www.michalson.com

Migiro, S., & Magangi, B. (2011). Mixed methods: A review of the literature and the future of the new research paradigm. *African Journal of Business Management, 5(10)*, 3757-3764.

Mitchell, R. C., Marcella, R., & Baxter, G. (1999). Corporate information security management. *New Library World, 100(5)*, 213-227.

Morgan, R. M., & Hunt, S. D. (1994). The commitment–trust theory of relationship marketing. *Journal of Marketing, 58*, 20-38.

Moyo, P. (2012). *Zimbabwe crafting new ICT policy.* Retrieved August 3, 2012, from http://www.itwebafrica.com/ict-and-governance/273-zimbabwe/229742-zimbabwe-crafting-new-ict-policy

Myers, M. D. (2009). *Qualitative research in business & management.* Los Angeles: Sage Publications.

Myers, M. D., & Avison, D. (2002). An introduction to qualitative research in information systems. Retrieved August 12 from http://eprints.soton.ac.uk/id/eprint/35818

Myers, M. D., & Klein, H. K. (2011). A set of principles for conducting critical research in information systems. *MIS Quarterly, 35(1)*, 17-36.

Myers, M. D., & Tan, F. B. (2002). Beyond models of national culture in information systems research. *Journal of Global Information Management, 10(2)*, 14-29.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules: An empirical study. *European Journal of Information Systems, 18(2),* 126-139.

Ngwenyama, O. K., & Lee, A. S. (1997). Communication richness in electronic mail: Critical social theory and the contextuality of meaning. *MIS Quarterly, 21(2)*, 145-167.

Nunnally, J. C. (1967). *Psychometric theory*. New York: McGraw-Hill.

Nyanchama, M. (2005). Enterprise vulnerability management and its role in information security management. *Information Systems Security, 14*(3), 29-56.

Onwuegbuzie, A. J., & Leech, N. L. (2004). Enhancing the interpretation of "significant" findings: The role of mixed methods research. *The Qualitative Report, 9(4)*, 770-792.

Oost, D., & Chew, E. (2007). Investigating the concept of information security culture. Retrieved August 12, 2012 from http://www.business.uts.edu.au/management/workingpapers/files/Oost2007.pdf

Oosthuizen, M., & Bhorat, H. (2004). *The post-apartheid South African labour market.* Retrieved February 20, 2012. Retrieved August 10, 2012 from http://www.tips.org.za/files/The_post_apartheid_SA_Labour_market_oosthuizen_Bhorat.pdf

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information Systems Research, 2(1)*, 1–28.

O'Reilly, C. A., & Chatman, J. A. Culture as social control: corporations, cults, and commitment. *Research in Organizational Behaviour, 18,* 157-200.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). *Employees' behavior towards IS security policy compliance*. Proceedings of the 40th Hawaii International Conference on System Sciences. Retrieved August 10, 2012 from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4076692

Pang, F., Sharma, R., Lederman, R., & Dreyfus, S. (2010). *Organisational culture and organisational impacts of information systems: A review of the empirical literature.* Paper presented at the 2010 ACIS Conference. Retrieved June 12, 2012 from http://aisel.aisnet.org/acis2010/96

Peltier, T. R. (2005). *Information security risk analysis.* Boca Raton: Auerbach Publications.

Pettigrew, A. M. (1979). On studying organizational culture. *Administrative Science Quarterly, 24,* 570-581.

Pfleeger, C. P. (1997). *Security in computing.* NJ: Prentice Hall.

Poverty Reduction and Economic Management (PREM). (2010). Africa's trade in services and economic partnership agreements. Retrieved August 10, 2012 from https://openknowledge.worldbank.org/bitstream/handle/10986/2942/557470ESW0Gray12B01PUBLIC0111221101.pdf?

Rees, P. L. (1993). User participation in expert systems. *Industrial Management & Data Systems, 93(6),* 3-7.

Reichardt, C. S., & Rallis, S. F. (1994). The qualitative-quantitative debate: New perspectives. *New Directions for Program Evaluation, 61*, 1-98.

Richardson, R. (2008). CSI computer crime and security survey. Retrieved August 10, 2012 from https://www.hlncc.com/docs/CSIsurvey2008.pdf

Robbins, S. P. (1989). *Organizational behaviour: Concepts, controversies, and applications* (4th ed.). New Jersey: Prentice Hall.

Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. *Information Management Journal, 39*(4), 60-66.

Salganik, M., & Heckathorn, D. D. (2004). Sampling and estimation in hidden populations using respondent-driven sampling. *Sociological Methodology, 34,* 193-239.

Schlienger, T., & Teufel, S. (2003). Analyzing information security culture: Increased trust by an appropriate information security culture. *Database and Expert Systems Applications, 2003. Proceedings. 14th International Workshop on,* 405-409.

Schein, E. H. (1985). *Organizational culture and leadership.* San Francisco: Jossey-Bass

Schein E. H. (1992). *Organisational culture and leadership (2nd ed.)* San Francisco: Jossey-Bass.

Schmidt, M. B., Johnston, A.C., Arnett, K.P., Chen, J.Q., & Li, S. (2008). A cross-cultural comparison of U.S and Chinese computer security awareness. *Journal of Global Information Management, 16(2),* 91-103.

Schneier, B. (2008). The psychology of security. Retrieved 23 November 2012 from http://www.schneier.com/essay-155.html

Shore, B., & Venkatachalam, A. R. (1996). Role of national culture in the transfer of information technology. *Journal of Strategic Information Systems, 5(1),* 19-36.

Schultz, E. (2005). The human factor in security. *Computers & Security, 24(6),* 425-426.

Scott, W. R. (1990). Innovation in medical care organizations: A synthetic review. *Medical Care Research Review, 47,* 165-192.

Sekaran, U. (2003). *Research methods for business: A skill-building approach.* New York: Wiley.

Siponen, M. T. (2000a). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8(1),* 31-41.

Siponen, M. T. (2000a). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8(1),* 31-41.

Siponen, M. T. (2005). Analysis of modern IS security development approaches: Towards the next generation of social and adaptable ISS methods. *Information and Organization, 15(4),* 339-375.

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *ACM Sigmis Database, 38(1),* 60-80.

Snijders, T. (1992). Estimation on the basis of snowball samples: How to weight. *Bulletin Methodologie Sociologique, 36,* 59-70.

Spears, J. L. (2006). The effects of user participation in identifying information security risk in business processes. *Proceedings of the 2006 ACM SIGMIS CPR Conference on Computer Personnel Research: Forty Four Years of Computer Personnel Research: Achievements, Challenges & the Future,* 351-352.

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly, 34(3),* 503.

Stahl, B. C., & Brooke, C. (2008). The contribution of critical IS research. *Communications of the ACM, 51(3),* 51-55.

Stan, S. (2007). Beyond information security awareness training: It is time to change the culture. Retrieved August 10, 2012 from http://www.citadel-information.com/wp-

content/uploads/2010/12/Beyond-Awareness-Training-Its-Time-to-Change-the-Culture-Stahl-0504.pdf

Standage, T. (2002). The weakest link. *Economist, 365(8296)*, 11-16.

Stanton, Jeffrey and Stam, Kathryn. (2006). *The visible employee: Electronic monitoring and information security*. Paper presented at the 2006 AMCIS Conference, Acapulco, Mexico. Retrieved May 21, 2012 from http://aisel.aisnet.org/amcis2006/407

Steele, S., & Wargo, C. (2007). An introduction to insider threat management. *Information Systems Security, 16(1)*, 23-33.

Steers, R. M., Meyer, A. D., Sanchez-Runde, C. J. (2008). National culture and the adoption of new technologies. *Journal of World Business, 43,* 255-260.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems. *Nist Special Publication, 800*-30.

Straub, D., Loch, K, Evaristo, J. R., Karahanna, E., & Srite, M. (2002). Toward a theory-based measurement of culture. *Journal of Global Information Management*, *10(1),* 13-23.

Straub, D. W., & Straub, W. (1990). Effective IS security. *Information Systems Research, 1*(3), 255-276.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22(4),* 441-469.

Subramanyam, R., Weisstein, F. L., & Krishnan, M. (2010). User participation in software development projects. *Communications of the ACM, 53(3)*, 137-141.

Suh, B., & Han, I. (2003). The IS risk analysis based on a business model. *Information & Management, 41(2)*, 149-158.

Sun, L., Srivastava, R.P., & Mock, T.J. (2006). An information systems security risk assessment model under the Dempster-Shafer theory of belief functions. *Journal of Management Information Systems, 22(4),* 109-142.

Tan, B., & Teo, T. (2000). Factors influencing the adoption of internet banking. *Journal of the Association for Information Systems, 1(5),* 1-42.

Tan, B., Watson, R., & Wei, K. K. (1995). National culture and group support systems: Filtering communication to dampen power differentials. *European Journal of Information Systems, 4(2)*, 82-92.

Terry, J., & Standing, C. (2004). The value of user participation in e-commerce systems development. *Informing Science, 7*, 31-45.

Tessina, T.B. (2008). What is dysfunctional relationship? Retrieved August 3, 2012 from http://tinatessina.com/dysfunctional_relationship.html

Thompson, L., & Spanier, G. B. (1983). The end of marriage and acceptance of marital termination. *Journal of Marriage and the Family, 45*, 103-113.

Thomson, K. L., von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security, 10,* 7-11.

Tong, C.K.S., Fung, K.H., Huang, H.Y.H., & Chan, K.K. (2003), Implementation of ISO17799 and BS7799 in picture archiving and communication system: Local experience in implementation of BS7799 standard. *International Congress Series, 1256,* 311-318.

Trompenaars, F., & Hampden-Turner, C. (1998). *Riding the waves of culture: Understanding diversity in global business*. NY: McGraw-Hill.

Tsiakis, T., & Stephanides, G. (2005). The economic approach of information security. *Computers & Security, 24*(2), 105-108.

Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008). Process-variance models in information security awareness research. *Information Management & Computer Security, 16*(3), 271-287.

Van Niekerk, J., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security, 29*(4), 476-486.

Vedder, K. (1998). International standardisation of IT security. *State of the Art in Applied Cryptography,* , 353-365.

Von Solms, B. (2000). Information security—the third wave? *Computers & Security, 19*(7), 615-620.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security, 23*(3), 191-198.

Walsham, G. (2006). Doing interpretive research. *European Journal of Information Systems, 15*(3), 320-330.

Wang, Q. H., & Kim, S. H. (2009). Cyber attacks: Cross-country interdependence and enforcement. *Eighth Workshop on the Economics of Information Security (WEIS 2009),*

Wang, R. Y., & Strong, D. M. (1996). Beyond accuracy: What data quality means to data consumers. *Journal of Management Information Systems,* , 5-33.

William & Hash (2003). Building an Information Technology Security Awareness and Training Program. Retrieved August 20, 2012 from http://mail.iwar.org.uk/comsec/resources/security-awareness/sp800-50.pdf

Whitman, M. E. (2008). SECURITY POLICY. *Information Security: Policy, Processes, and Practices, 11*, 123.

Yum, Y., & Hara, K. (2006). Computer-Mediated relationship development: A Cross-Cultural comparison. *Journal of Computer-Mediated Communication, 11*(1), 133-152.

Zafar, H., & Clark, J. G. (2009). Current state of information security research in IS. *Communications of the Association for Information Systems, 24*(1), 557-596.

Zmud, R. W. (1978). An empirical investigation of the dimensionality of the concept of information. *Decision Sciences, 9*(2), 187-195.

Chapter 7 : Appendices

Appendix A: Interview Guide

A. Demographic details

1. What is the name of your organisation?
2. How long have you worked for this organisation?
3. What is your position or responsibility in the organisation?
4. What is your highest professional qualification?
5. Have you held any other position a part from the current one?
6. How long have you been at your current position? (Number of Years)

B. Knowledge about Information Security Risk Management

7. What level of knowledge do you have on Information Technology (IT)?
8. What training (if any) have you attended relating to Information Security?
9. What do you understand by the terms Information Security, or Information Security Risk Management?
10. How would you differentiate the terms Information Security and Information Security Risk Management?
11. Have there been information security awareness campaigns in your organisation? (If No, skip to 13)
12. How often are these campaigns conducted?
13. What roles or activities are within the scope of Information Security Risk Management?
14. What roles or tasks are performed by users that are within the scope of Information Security Risk Management?
15. What roles are performed by users when the organisation analyses Information Security Risks?

C. Participation of users in Information Security Risk Management through daily information security control

16. Have users in your organisation actively participated in following roles associated with Information Security Control?
    (a) Granting access rights to information and information systems
    (b) Separation or segregation of duties
    (c) Definition of alerts, triggers or application controls
    (d) Analysis of exception reports
    (e) Participating on organisation-wide Information Security awareness campaigns
    (f) Determining risk levels which can be tolerated

D. Participation of users in Information Security Risk Management via accountability roles

17. During the past 12 months, have users in your organisation been assigned roles associated with management and accountability of roles such as the following?
    (a) Definition and documentation of roles and responsibilities
    (b) Assignment of roles and responsibilities for protection information resources
    (c) Data of process owners (business users) made responsible for specific controls
    (d) Reviews of Information Security policy
    (e) Communication of Information Security policy to all other employees
    (f) User support demonstrated for information security
    (g) Information Security Risk Management planning

E. Awareness of security policies and procedures

18. Do you agree with the statement that users working with information in your organisation have increased awareness of information security policies, procedures and the need to ensure data integrity?
    (a) Strongly disagree (people most often need to be reminded to follow information security policy)
    (b) Moderately agree (many people seem aware, while many others do not seem to be aware)
    (c) Strongly agree (people often mention or ask questions to clarify, what is needed for information security)

F. Demonstrated sense of ownership

19. Do you agree with the statement that users who handle information have demonstrated a sense of ownership towards protecting the information integrity in the past 12 months?
    (a) Strongly disagree (users often need to be reminded to comply with information security controls or policies)
    (b) Agree and disagree (many users take ownership while many do not)
    (c) Strongly agree (most users are proactive in taking responsibility for information security)

G. Control development and remediation

20. Have functional users actively contributed in security control development and remediation by performing any of the following
    (a) Provide information needed by control designers?
    (b) Documentation of decision criteria for granting access to information systems?
    (c) Assessment of controls to identify those controls which need remediation?

H. Perceived improvement in control development

21. Has there been an improvement in the definition or implementation of each of the following:
    (a) Access control for system users?
    (b) Segregation of duties for system users?
    (c) Information security policy?

I. Control performance via reduced deficiencies

22. Total number or magnitude of control deficiencies for key controls has decreased in the past 12 months?
    (a) Strongly disagree (control deficiencies are much worse)
    (b) Agree and disagree (total number or magnitude decreased/increased)
    (c) Strongly agree (major improvement)

J. Control performance via increased efficiencies

23. To what degree have there been efficiency improvements made to the system of controls, by redesigning, consolidating, or automating key controls used to manage risks to information systems?
    (a) Much worse (important controls stopped, weakening security or controls very inefficient)
    (b) No change
    (c) Much better (a major focus in the organisation; extensive improvements made)

Appendix B: Questionnaire

Understanding the effects of user participation in Information Security Risk Management: A comparative study of South Africa and Malawi

Questionnaire Instrument

Demographic Details

1. What is the name of your organisation?
   _____
2. In which industry is your organisation?
   _____
3. Which region do you consider your primary residence?
   _____
4. Enter the city/town where you operate?
   _____
5. What is your position or responsibility in this organisation?
   _____
6. How long (in years) have you been working on your current position?
   _____
7. What is your highest educational/professional qualification?
   _____

Knowledge about Information Security Risk Management

1. What level of knowledge do you have on Information Technology (IT)?
   1. Novice (minimal knowledge of IT) ( )
   2. Advanced beginner (working knowledge of IT still limited but recognisable after some experience) ( )
   3. Competent (good working and background knowledge of IT) ( )
   4. Proficient (deep understanding and practice of IT) ( )
   5. Expert (authoritative knowledge and deep tacit understanding and practice of IT) ( )
2. What level of knowledge do you have on information security and/or information security risk management (ISRM)?
   1. Novice (minimal knowledge of ISRM) ( )
   2. Advanced beginner (working knowledge of ISRM still limited but recognisable after some experience) ( )
   3. Competent (good working and background knowledge of ISRM) ( )
   4. Proficient (deep understanding and practice of ISRM) ( )
   5. Expert (authoritative knowledge and deep tacit understanding and practice of ISRM) ( )
3. What training (if any) have you attended that relates to information security risk management?
   _____

4. What roles or activities are within the scope of Information Security Risk Management? (Enter each role/activity on a separate line)

   _____
   _____

5. What roles are performed by users in your organisation which signify their participation in Information Security Risk Management? (Enter each role or activity on a separate line)

   _____
   _____

6. Does your organisation conduct any information security awareness campaigns?
   1. Yes ( )
   2. No ( )
   3. Don't know ( )

7. If yes to the previous question, how often are these campaigns conducted?

   _____

Information Security Risk Management

1. In managing Information Security risks, do users in your organisation actively perform or contribute to decision-making in any of the following Information Security Risk Management activities?

   1.1. Documenting business processes or transactions for risk evaluation
   1. Yes ( )
   2. No ( )
   3. Don't know ( )

   1.2. Ensuring key controls exist to mitigate specific types of risks
   1. Yes ( )
   2. No ( )
   3. Don't know ( )

   1.3. Defining procedural controls for example rules for access control
   1. Yes ( )
   2. No ( )
   3. Don't know ( )

   1.4. Implementing controls
   1. Yes ( )
   2. No ( )
   3. Don't know ( )

   1.5. Reviewing and testing controls
   1. Yes ( )
   2. No ( )
   3. Don't know ( )

   1.6. Remediating defective controls
   1. Yes ( )

2. No ( )
3. Don't know ( )

1.7. Communicating Information Security regulatory initiatives
1. Yes ( )
2. No ( )
3. Don't know ( )

Information Security Controls

2. Have users in your organisation actively participated in defining, reviewing, or approving any of the following which relates to Information Security Control?

2.1. Granting access to information resources

1. Yes ( )
2. No ( )
3. Don't know ( )

2.2. Separation (segregation) of duties

1. Yes ( )
2. No ( )
3. Don't know ( )

2.3. Definition of alerts, triggers, or application controls

1. Yes ( )
2. No ( )
3. Don't know ( )

2.4. Analysis of exception reports

1. Yes ( )
2. No ( )
3. Don't know ( )

2.5. Participating in Information Security awareness campaigns

1. Yes ( )
2. No ( )
3. Don't know ( )

2.6. Determining risk tolerance (risk acceptance level)

1. Yes ( )
2. No ( )
3. Don't know ( )

Accountability Roles

3. During the past 12 months, have any of the following activities occurred in your organisation which provide accountability roles to users for Information Security Risk Management?

   3.1. Individual roles and responsibilities defined and documented
   1. Yes ( )
   2. No ( )
   3. Don't know ( )

   3.2. Roles and responsibilities for protecting information assigned
   1. Yes ( )
   2. No ( )
   3. Don't know ( )

   3.3. Users (data or process owners) made responsible for specific controls
   1. Yes ( )
   2. No ( )
   3. Don't know ( )

   3.4. Reviews of Information Security Policy
   1. Yes ( )
   2. No ( )
   3. Don't know ( )

   3.5. Information Security Policy communicated to all other users and stakeholders
   1. Yes ( )
   2. No ( )
   3. Don't know ( )

   3.6. Management support demonstrated for Information Security
   1. Yes ( )
   2. No ( )
   3. Don't know ( )

   3.7. Information Security planning
   1. Yes ( )
   2. No ( )
   3. Don't know ( )

Awareness and sense of ownership

4. "Users working with information have increased awareness of policies, procedures and the need to ensure information security"

   1. Strongly disagree (users often need to be reminded to follow security policy) ( )
   2. Disagree ( )
   3. Neutral (Not certain) ( )
   4. Agree ( )

5. Strongly agree (users often ask for clarification on the information security policy) ( )

5. "During the past 12 months, users in your organisation who handle information have demonstrated a sense of ownership toward protecting the information integrity"

1. Strongly disagree (users are often reminded about Information Security Policy) ( )
2. Disagree ( )
3. Neutral (Not certain) ( )
4. Agree ( )
5. Strongly agree (users proactively take responsibility for information security) ( )

6. During the past 12 months, users in your organisation have actively contributed in security control development and remediation by performing any of the following actions:

6.1. Provide information needed by control designers

1. Yes ( )
2. No ( )
3. Don't know ( )

6.2. Documentation of criteria for granting access to information systems

1. Yes ( )
2. No ( )
3. Don't know ( )

6.3. Assessment of controls to identify those which need remediation

1. Yes ( )
2. No ( )
3. Don't know ( )

7. To what extent has there been an improvement (if any) in the definition or implementation of each of the following as part of your organisation's Information Security Risk Management efforts?

7.1. Access control for system users

1. Much worse ( )
2. Worse ( )
3. No change ( )
4. Better ( )
5. Much better ( )

7.2. Segregation of duties for system users

1. Much worse ( )
2. Worse ( )
3. No change ( )
4. Better ( )
5. Much better ( )

7.3. Information Security Policy

1. Much worse ( )
2. Worse ( )
3. No change ( )
4. Better ( )
5. Much better ( )

8. "During the past 12 months, the total number or magnitude of control deficiencies for key controls has decreased signifying improvement in control efficiencies"

1. Strongly disagree (increased number or magnitude of control deficiencies) ( )
2. Disagree ( )
3. Neutral (no change) ( )
4. Agree ( )
5. Strongly agree (decreased number or magnitude of control deficiencies) ( )

9. To what degree have there been efficiency improvements made to the system of controls by redesigning, consolidating, or automating key controls used to manage Information Security risk?

1. Much worse (weak controls are stopped thereby weakening security further) ( )
2. Worse ( )
3. Neutral (no improvement) ( )
4. Better ( )
5. Much better (a major focus in the organisation; extensive improvements made) ( )

***** End of questionnaire *****

Appendix C: Letter of Introduction

Department of Information Systems
Leslie Commerce Building
Engineering Mall, Upper Campus
Private Bag. Rondebosch 7701
Cape Town
Tel: (021) 650-2261
Fax No: (021) 650-2280

Masters Dissertation: Participant Consent Form

Dear Sir/Madam,

I am an Information Systems Masters student at the University of Cape Town. I am conducting a case study to assess the impact of user participation in Information Security Risk Management (ISRM).

As part of the research process, I will be conducting interviews with some members of staff at "organisation" to gain an understanding on user participation roles in ISRM. Your participation in this research is greatly appreciated.

The questions for the interview have been approved by the University's Ethics committee. Please note that participation is voluntary and that all data collected will be treated as confidential. The findings from the study will be kept anonymous and will be published as part of the research. If you are interested to receive a copy of the final report of the research, you are welcome to provide your email address and the results will be sent to you.

If you have any further queries, please feel free to contact either the researcher or Prof. Michael Kyobe. Contact details are provided below.

Thank you for your time and cooperation

Sincerely,

Masters Student (Information Systems):

Researcher : Dimson Kalelo-Phiri klldim001@uct.ac.za : _____

Supervisor : Prof. Michael Kyobe Michael.Kyobe@uct.ac.za : _____

Department of Information Systems
University of Cape Town

PARTICIPANT CONSENT FORM

By signing this form, you are agreeing to participate in the research project entitled "Understanding the effects of user participation in Information Security Risk Management: A comparative study of South Africa and Malawi"

Signature : _____ Date : _____

Appendix D: Factor extraction

Rotated Component Matrix[a]									
Questionnaire Items	**Components**								
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Q1.1: Documenting business processes or transactions for risk evaluation	.755								
Q1.2: Ensuring key controls exist to mitigate specific types of risks				.599					
Q1.3: Defining procedural controls (rules for access control)	.808								
Q1.4: Implementing controls	.770								
Q1.5: Reviewing and testing controls	.508			.679					
Q1.6: Remediating defective controls				.690					
Q1.7: Communicating Information Security regulatory initiatives	.772								
Q2.1: Granting access to information resources			.523						
Q2.2: Separation (segregation) of duties			.838						
Q2.3: Definition of alerts, triggers, or application controls			.737						
Q2.4: Analysis of exception reports			.668					.528	
Q2.5: Participating in Information Security awareness campaigns							.636		
Q2.6: Determining risk tolerance (risk acceptance level)			.607						
Q3.1: Individual roles and responsibilities defined and documented				.630					
Q3.2: Roles and responsibilities for protecting information assigned								.504	
Q3.3: Users (data or process owners) made responsible for specific controls				.756					
Q3.4: Reviews of information security policy		-.625							
Q3.5: Information Security Policy communicated to all other users and stakeholders							.834		
Q3.6: Management support demonstrated for Information Security					.687				
Q3.7: Information security planning									
Q4: User increased awareness of policies, procedures and the need for information security						.984			
Q5: User demonstrated a sense of ownership toward protecting the information integrity						.983			
Q6.1. Provide information needed by control designers					.729				
Q6.2: Documentation of criteria for granting access to information systems					.854				
Q6.3: Assessment of controls to identify those which need remediation.					.539				
Q7.1: Access control for system users		.857							
Q7.2: Segregation of duties for system users		.803							
Q7.3: Information Security Policy		.762							
Q8: Decreased number of control deficiencies for key controls		.717							
Q9: Efficiency improvements made to the system of controls									.729

Appendix E: List of utility companies in Malawi

Type	Companies
Water supply	• Blantyre Water Board (BWB) • Central Region Water Board (CRB) • Eastern Region Water Board (ERWB) • Lilongwe Water Board (LWB) • Mzuzu Water Board (MWB) • Northern Region Water Board (NWB) • Southern Region Water Board (SRWB)
Electricity	• Electricity Supply Commission of Malawi (ESCOM)
Mobile phone operators	• Airtel • Malawi Telecommunications Limited (MTL) • Telecom Networks Malawi (TNM) • Access

Appendix F: Research time plan

Due Date	Duration (months)	Activity	Deliverable
19 May, 2011		Research proposal writing	Research proposal
25th July, 2011	2	Literature review	Literature review report
30th Sep, 2011	2	Research design	Research design
30th Nov, 2011	1	Review of study instruments	Study instruments
15th May, 2012	3	Data collection, analysis and interpretation of results	
30th May, 2012	0.5	Thesis writing	Thesis draft
15th June, 2012	0.5	Thesis writing	Revised thesis draft
15th Aug, 2012	1	Thesis writing	Thesis completed version