INFORMATION SECURITY RISK MANAGEMENT IN SMALL-SCALE ORGANISATIONS: A CASE STUDY OF SECONDARY SCHOOLS' COMPUTERISED INFORMATION SYSTEMS.

by

MOSES MOYO

submitted in accordance with the requirements for
the degree of

MASTER OF SCIENCE

in the subject

INFORMATION SYSTEMS

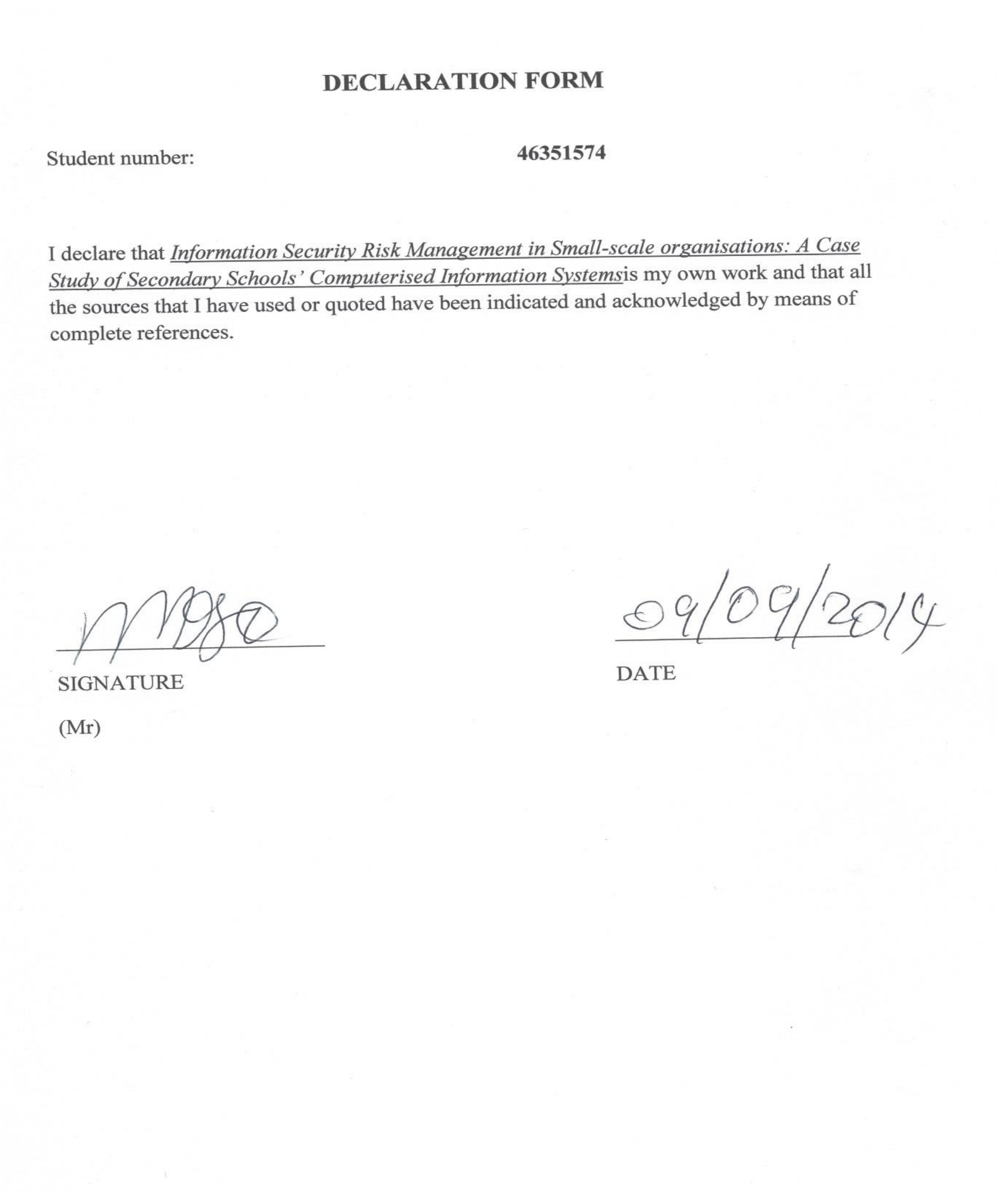
at the

UNIVERSITY OF SOUTH AFRICA

Supervisor:	Ms Hanifa Abdullah
Co-Supervisor:	Dr Rita C. Nienaber

February 2014

DECLARATION FORM



DECLARATION FORM

Student number: **46351574**

I declare that *Information Security Risk Management in Small-scale organisations: A Case Study of Secondary Schools' Computerised Information Systems*is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

SIGNATURE

(Mr)

09/09/2014

DATE

DEDICATION

I dedicate this dissertation to my wife Primrose and family

ACKNOWLEDGEMENTS

I would like to thank my immediate family members for their support during the course of this research study. Secondly, I want to thank my supervisors Ms Abdullah H and Dr Nienaber RC for their tireless effort and guidance throughout the study

I also thank the principals and educators I worked with during the data collection process. I extend my gratitude to the Vhembe District, Department of Education for permitting me to carry out the research in their schools.

Finally, I thank all my friends who gave me support throughout this study.

Thank you.

ABSTRACT

Threats to computerised information systems are always on the rise and compel organisations to invest a lot of money and time amongst other technical controls in an attempt to protect their critical information from inherent security risks. The computerisation of information systems in secondary schools has effectively exposed these organisations to a host of complex information security challenges that they have to deal with in addition to their core business of teaching and learning. Secondary schools handle large volumes of sensitive information pertaining to educators, learners, creditors and financial records that they are obliged to secure. Computerised information systems are vulnerable to both internal and external threats but ease of access sometimes manifest in security breaches, thereby undermining information security. Unfortunately, school managers and users of computerised information systems are ignorant of the risks to their information systems assets and the consequences of the compromises that might occur thereof. One way of educating school managers and users about the risks to their computerised information systems is through a risk management programme in which they actively participate. However, secondary schools do not have the full capacity to perform information security risk management exercises due to the unavailability of risk management experts and scarce financial resources to fund such programmes.

This qualitative case study was conducted in two secondary schools that use computerised information systems to support everyday administrative operations. The main objective of this research study was to assist secondary schools that used computerised information systems to develop a set of guidelines they would use to effectively manage information security risks in their computerised information systems. This study educated school managers and computerised information systems users on how to conduct simple risk management exercises. The Operationally Critical Threats, Assets and Vulnerability Evaluation for small-scale organisations risk management method was used to evaluate the computerised information systems in the two schools and attain the goals of the research study. Data for this study were generated through participatory observation, physical inspections and interview techniques. Data were presented, analysed and interpreted qualitatively.

This study found that learners’ continuous assessment marks, financial information, educators’ personal information, custom application software, server-computers and telecommunication equipment used for networking were the critical assets. The main threats to these critical assets were authorised and unauthorised systems users, malware, system crashes, access paths and incompatibilities in software. The risks posed by these threats were normally led to the unavailability of critical information systems assets, compromise of data integrity and confidentiality. This also led to the loss of productivity and finance, and damage to school reputation. The only form of protection mechanism enforced by secondary schools was physical security. To mitigate the pending risks, the study educated school managers and users in selecting, devising and implementing simple protection and mitigation strategies commensurate with their information systems, financial capabilities and their level of skills. This study also recommended that secondary schools remove all critical computers from open-flow school networks, encrypt all critical information, password-protect all computers holding critical information and train all users of information systems of personal security.

The study will be instrumental in educating school managers and computerised information systems users in information security awareness and risk management in general.

LIST OF ABBREVIATIONS

Table 0.0: List of important abbreviations used

ABBREVIATION	DESCRIPTION
ACTIA	Australian Capital Territory Insurance Authority
AIRMIC, ALARM & IRM	The Association of Insurance and Risk Managers, The National Forum for Risk Management and The Institute of Risk Management
ALE	Annualised Loss Expectancy
AS/NZ 4360:2004	The Australian and New Zealand Standards on Risk Management: 2004.
AS/NZS ISO 31000:2009	Australian/New Zealand Standard™ Risk management principles and guidelines
AVG	Antivirus guard
CISs	Computerised information systems
COBRA	Consultative, Objective and Bi-functional Risk Analysis
CRAMM	Central Computer and Telecommunications Agency Risk Analysis and Management Method (CRAMM)
CVE	Common vulnerabilities and exposures
DEAT	Department of Environmental Affairs and Tourism
DoE	Department of Education
DoS	Denial of Services
FET	Further Education and Training
FHWA	Federal Highway Administration
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode and Effects Criticality Analysis
GFI	Galea Francheschini Innovation
HAZOP	Hazard And Operability study
LAN	Local area networks
LRAM	Livermore Risk Analysis Methodology
MAC	Media access control
NOWECO	Northwest Controlling Corporation L.t.d
NTRSA	National Treasury Republic of South Africa
OCTAVE	The Operationally Critical Threat, Asset and Vulnerability Evaluation

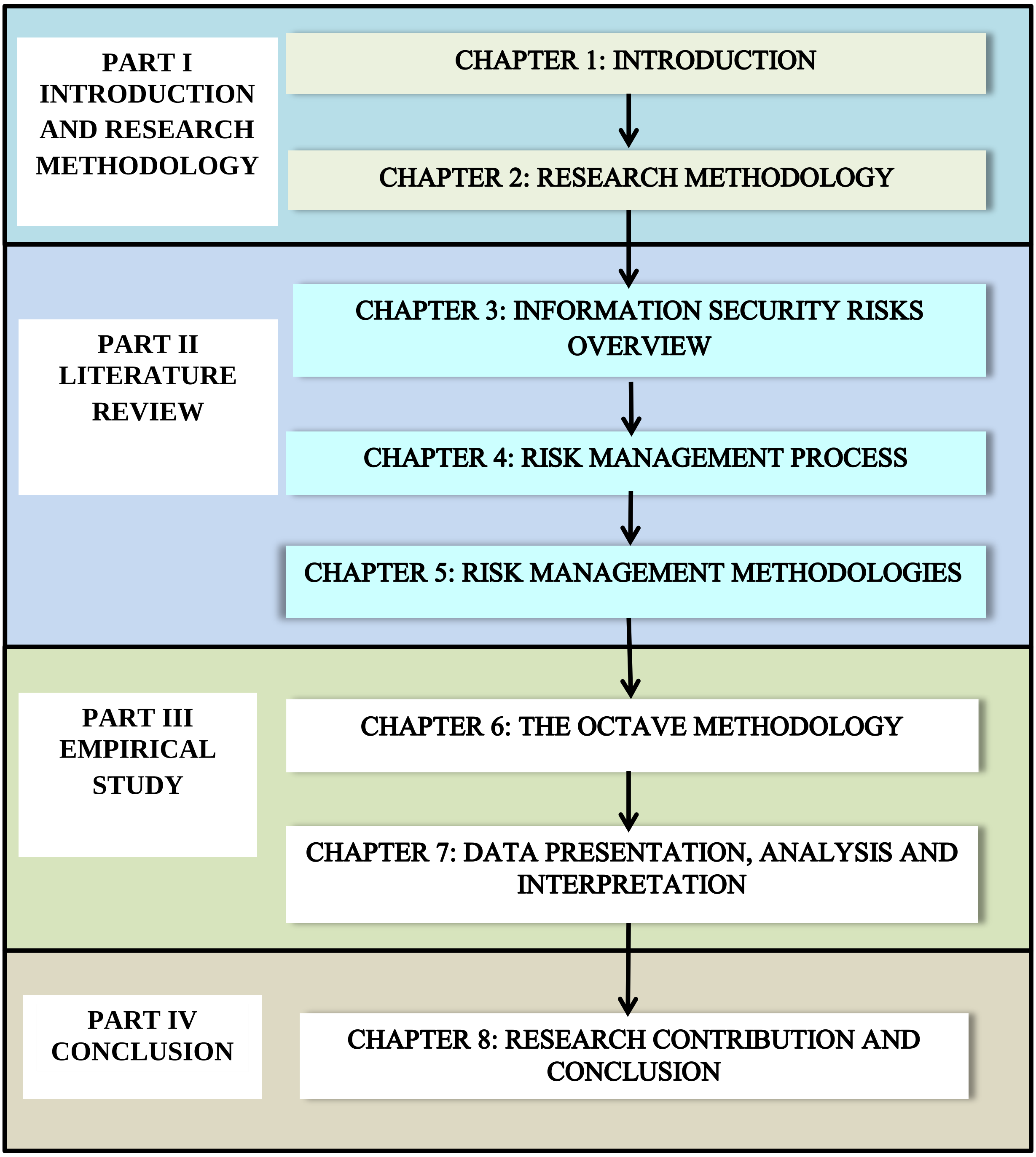
ABBREVIATION	**DESCRIPTION**
OSY	United States Department of Commerce Office of Security
TSQ	The State of Queensland
USDHS	United States of America Department of Home Security
GAO/AIMD	United States Government Accountability Office
Sacfis	South African Centre for Information Security

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

DISSERTATION CHAPTERS LAYOUT



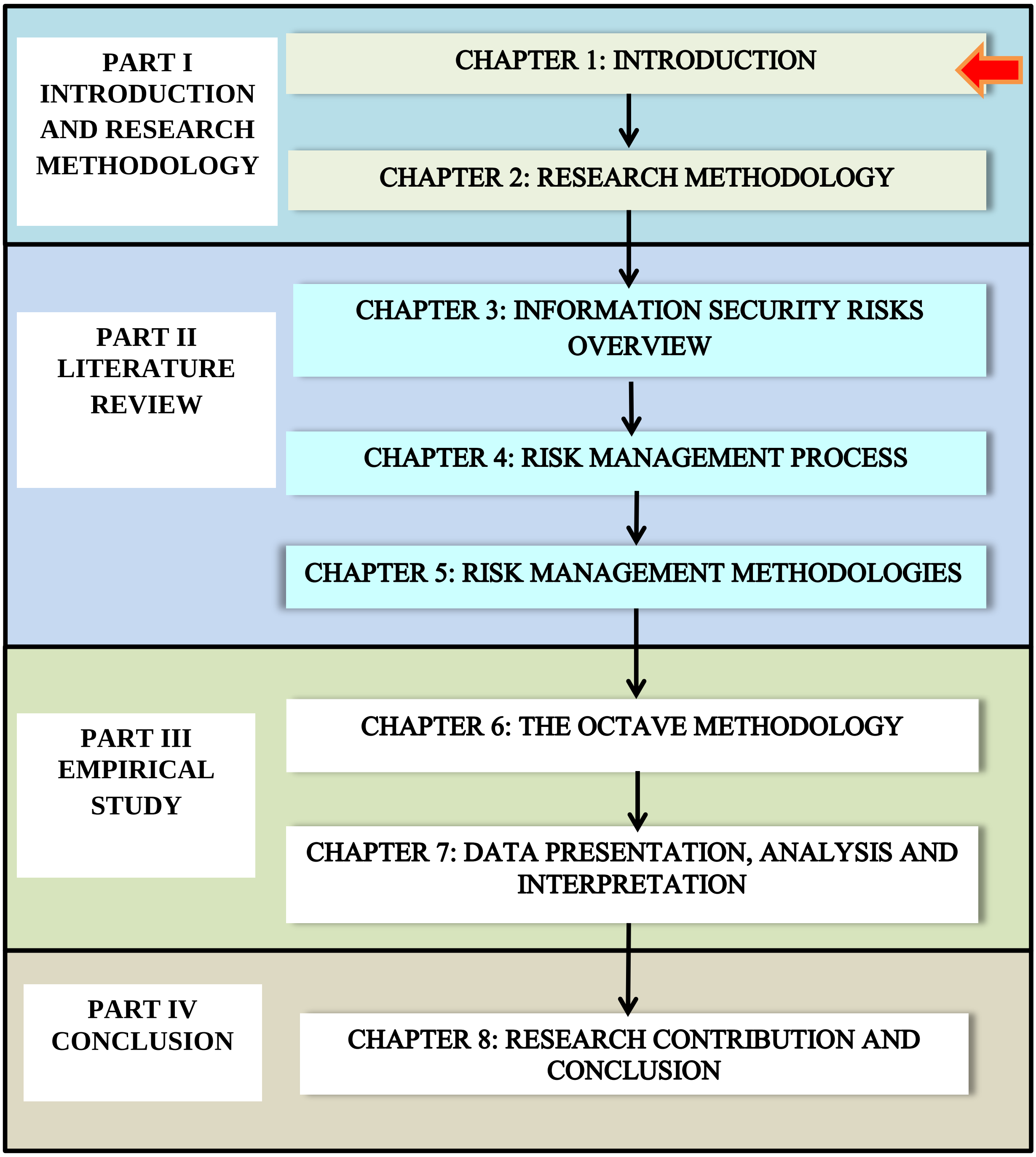
PART I
INTRODUCTION AND RESEARCH METHODOLOGY
CHAPTER 1: INTRODUCTION
CHAPTER 2: RESEARCH METHODOLOGY
PART II
LITERATURE REVIEW
CHAPTER 3: INFORMATION SECURITY RISKS OVERVIEW
CHAPTER 4: RISK MANAGEMENT PROCESS
CHAPTER 5: RISK MANAGEMENT METHODOLOGIES
PART III
EMPIRICAL STUDY
CHAPTER 6: THE OCTAVE METHODOLOGY
CHAPTER 7: DATA PRESENTATION, ANALYSIS AND INTERPRETATION
PART IV
CONCLUSION
CHAPTER 8: RESEARCH CONTRIBUTION AND CONCLUSION

PART I

INTRODUCTION AND RESEARCH METHODOLOGY

CHAPTER 1

1. INTRODUCTION


PART I INTRODUCTION AND RESEARCH METHODOLOGY
CHAPTER 1: INTRODUCTION
CHAPTER 2: RESEARCH METHODOLOGY
PART II LITERATURE REVIEW
CHAPTER 3: INFORMATION SECURITY RISKS OVERVIEW
CHAPTER 4: RISK MANAGEMENT PROCESS
CHAPTER 5: RISK MANAGEMENT METHODOLOGIES
PART III EMPIRICAL STUDY
CHAPTER 6: THE OCTAVE METHODOLOGY
CHAPTER 7: DATA PRESENTATION, ANALYSIS AND INTERPRETATION
PART IV CONCLUSION
CHAPTER 8: RESEARCH CONTRIBUTION AND CONCLUSION

1.1. INTRODUCTION

The ability of an organisation to fulfil its mission depends on the meaningful and productive utilisation of its assets (Anderson & Choobineha, 2008). Computerised information systems (CISs) are now common assets that South African secondary schools utilise to fulfil their missions in service delivery. These computerised information systems are exposed to information security risks and their survival depends on the quality and effectiveness of risk management programmes that secondary schools implement.

Risk management comprises of a number of steps of which risk assessment and analysis are the most important and focal ones (Karabacaka & Sogukpinar, 2003). The outcome of risk assessment and analysis plays an important role in risk management in an organisation that uses information systems (Jenkins, 1998; Alberts & Dorofee, 2001; Siu, 2007; Yeha & Chang, 2007). Management uses risk assessment and analysis outcomes to decide on whether to accept or mitigate identified information security risks. The choice of risk mitigation strategies by an organisation is a crucial step towards an organisation's quest to deploy, implement and manage its information security tools (Beachboard, Cole, Mellor, Hernandez & Aytes, 2008). The complexity of establishing completely secured information systems is an adequate contribution to the complications of information securities in secondary schools' CISs. There is no doubt that those secondary schools using CISs experience information security risk problems similar to other small-scale organisations. Lack of sound risk management programmes is cited as a major contributory factor to information systems security risks in small-scale organisations (Beachboard *et al*. 2008). The possibility of secondary schools overlooking this essential information security requirement is high. In the event of threat attacks occurring, secondary schools may be prompted to use unsanctioned risk management techniques or even be compelled to abandon the programmes altogether. This is likely to jeopardise CISs thereby affecting important administrative operations and overall service delivery. If this situation continues unabated, it can eventually have negative impact on secondary schools' administrative operations especially those that depend on CISs.

This qualitative case study was designed to assist secondary school managers and CISs users on developing guidelines that they would use to manage information security risks their CISs. The managers and users of CISs were to be educated on how to conduct information security risk management exercises using the Operationally Critical Threats, Assets and Vulnerability for small organisation (OCTAVE-small) risk management method. The study was carried out in two secondary schools in the Thohoyandou Cluster, Vhembe District, where CISs were being used.

This chapter serves as an introduction to the research study. The chapter is structured on subtopics covering different important aspects of the study. The introduction puts the research into perspective by highlighting the need for small-scale organisations to be proactive in addressing information security risks that affect their CISs. A preliminary literature review provides the background of the study and it briefly examines what has been already published in information security and risk management. The literature review is intended to inform the reader of the risk management frameworks and methodologies in use today, their merits and demerits as applied in various organisational contexts. The chapter then elucidates the motivation, research context and the problem statement of this research study. Research objectives which guide this study are stated immediately after the problem statement. Risk management methodologies, research strategy and data collection techniques to be adopted in this study are also briefly discussed. This chapter also examines research ethics in order to inform the readers how human beings (subjects) would be protected during data collection. The overall layout of the dissertation is also given to guide the reader on the number of chapters that constitute the dissertation and what each chapter covers. Important issues discussed in this chapter are summarised in the conclusion.

1.2. RESEARCH BACKGROUND

Rapid changes in computing technologies tend to have a bearing on computing environments in organisations which use CISs. Some of the changes are accompanied by positive information security results while others lead to a variety of security risks which adversely affect the existing information systems (Karabacaka & Sogukpinar, 2003). An organisation whose operations depend on CISs requires a secured computing environment to achieve its missions. Unlike in the past, where information security was the responsibility of information security experts, non-experts are now required to actively participate in creating secure computing environments for their organisations (Steve, 2007). This involves the development of a general understanding of information security risks and the application of risk management methodologies in work places (Karabacaka & Sogukpinar, 2003). Organisations which implement participatory risk management methodologies stand better chances of succeeding in countering risks (Alberts & Dorofee, 2003) than those relying on technical expertise only (Canavan, 2001; Doherty & Fulford, 2006; Caballero, 2009). Such organisations derive considerable benefits from their CISs. Secondary schools, may benefit from these methodologies if they properly implement information security risk management programmes initiated by school managers and users of CISs.

1.2.1. Information security

Information plays a vital role in the existence of any organisation and it should always be secured (Gerber & von Solms, 2001). The benefits of information security are in supporting the mission of an organisation to achieve its objectives (Stoneburner, Goguen & Feringa, 2002; Steve, 2007; Yeha & Chang, 2007). Information security is the protection of information systems against unauthorised access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorised users, including those measures necessary to detect, document, and counter such threats (Yeha & Chang, 2007). The major goal of information security in an organisation is to preserve the confidentiality, integrity and availability of information (Theoharidou, Kokolakis, Karyda & Kiountouzis, 2005). *Confidentiality* is the protection of information against theft and eavesdropping and *integrity* refers to the protection of information against unauthorised modification and masquerade (Elky, 2006). *Availability* is the dependable access of users to authorised information, particularly in light of attacks such as denial of service (DoS) against information systems (Chen, 2009). Information security requires a range of skills and knowledge that are rarely found in small-scale organisations such as secondary schools, an issue being addressed by this research study.

Research in information security indicates that small-scale organisations seldom deploy proper information security controls regardless of the availability of guidelines to this effect (Dimopoulos, Furnell & Barlow, 2003; Beachboard *et al*. 2008). Management in small-scale organisations are prepared to invest more resources in protecting computing infrastructure without assessing the risks to their critical information (Dimopoulos *et al*. 2003; Panda, 2009). Whether management in small-scale organisations deliberately prefer to protect computing infrastructure, or it is due to a lack of security risk management knowledge, the reason for this is yet to be established (Stoneburner *et al*. 2002, Siu, 2007; Steve, 2007). It seems that management in small-scale organisations, including secondary schools may have a narrower view or have no knowledge of information security. This may prohibit the prospects of conducting risk management programmes in these institutions.

1.2.2. Risk management

Risk management is a systematic and analytical process whereby an organisation identifies, reduces and controls its potential threats and losses (Stoneburner *et al*. 2002). According to Hoo (2000), risk management is a policy process wherein alternative strategies for dealing with risks are weighed and decisions about acceptable risks are made. A well-managed information system is always supported by a sound risk management plan intended to identify, reduce and maintain risks to acceptable levels (Yeha & Chang, 2007). Therefore, risk management is an on-going process that attempts to identify threats or reduce their impact whenever an attack occurs. Risk management is an iterative process with well-defined steps, which when taken in sequence, supports better decision-making by contributing a greater insight into risks and their impacts (Hoo, 2000). Large organisations include their risk management plans in their security policies (Alberts & Dorofee, 2001; Beachboard *et al*. 2008). This is different from small-scale organisations such as secondary schools that may have problems in formulating workable risk management plans and fail to implement them.

1.2.3. Risk management methods

Risk management methods can be quantitative or qualitative depending on the risk assessment and analysis applied (Mazareanu, 2007; Ganthan, Rabiah & Zuraini, 2009). These methods apply different techniques and therefore require different expertise. *Quantitative* risk management methods use numerical results that express the probability of each risk factor and its effects on the objectives of the organisation (Mazareanu, 2007). Popular examples of quantitative risk assessment and analysis methods are the Annualised Loss Expectancy (ALE) and the Livermore Risk Analysis Methodology (LRAM) (Rainer, Snyder & Carr, 1991; Elky, 2006; Beachboard *et al*. 2008). Quantitative methods are regarded as being more objective than qualitative methods because they depend on easily verifiable mathematical formulae (Rainer *et al*. 1991; Mazareanu, 2007). These methods are suitable for large information systems infrastructure supported by strong human and financial resources (Elky, 2006; Panda, 2009). Quantitative methods rely on estimations of the probability of damages or loss of information systems assets (Beachboard *et al*. 2008; Ding, 2002). This makes quantitative risk methods problematic to use in small-scale organisations such as secondary schools where there are no risk management experts to perform such complex estimations. A risk management exercise conducted using a quantitative method is generally more expensive and demands greater experience and advanced tools than those conducted using qualitative methods (Rot, 2008). Due to these constraints, small-scale organisations, such as secondary schools lack the capacity to use quantitative risk management methods, hence qualitative methods become an alternative.

Qualitative risk management assesses the effects of the identified risk factors and then creates priorities used to decide on how to solve the potential risk factors, depending on the impact they could have on the information systems (Panda, 2009). Most qualitative methods can be modified for easy use with any expertise available in an organisation (Panda, 2009). Generally, qualitative methods tend to be simpler to implement than quantitative methods because they express risks in terms of simple descriptive variables or adjectives instead of precise monetary terms, therefore, requiring less time, finance and effort to implement (Mazareanu, 2007). This argument arises from the fact that qualitative methods utilise the security jargon which non-technical people may be familiar with (Rainer *et al*. 1991; Mazareanu, 2007). Furthermore, qualitative methods are based on judgment, intuition and experience of the team that conducts the risk management exercise (Rainer *et al*. 1991). This makes qualitative risk management methods a better choice for use in secondary schools where there are no risk management personnel.

Popular examples of qualitative risk management methods are Hazard And Operability study (HAZOP), Failure Mode and Effects Analysis (FMEA) or Failure Mode and Effects Criticality Analysis (FMECA) and United Kingdom (UK) Government's Risk Analysis and Management Method (CRAMM) (Karabacaka & Sogukpinar, 2003; Yazar, 2004; Elyse, 2007; Panda 2009). Another example is Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) (Alberts & Dorofee, 2001; Panda, 2009). Some of these qualitative risk techniques pose serious problems in small-scale organisations in that they either require highly trained technical teams to perform risk assessment and analysis, are labour intensive or have strong financial basis (Karabacaka & Sogukpinar, 2003; Yazar, 2004; Elyse, 2007; Panda 2009). Secondary schools hardly have such expertise and financial bases to undertake such endeavours and as a result, this makes the use of these methods unaffordable and unsuitable for secondary schools. Contrary to some of the qualitative methods, the OCTAVE method does not require highly technical people or strong financial support to be implemented (Alberts & Dorofee, 2002; Alberts & Dorofee 2004; Panda, 2009). This is likely to make OCTAVE to be the most appropriate information security risk management method for use in organisations where there are no experts in information security risk management (Alberts & Dorofee, 2001; Panda, 2009).

The choice of a risk management method depends on the understanding and appropriate application of that method in a given organisational context (Mazareanu, 2007; Beachboard *et al*. 2008). This area is considered to be difficult particularly to resource and expertise-constrained small and medium-sized enterprises (Karabacaka & Sogukpinar, 2003: Siu, 2007). This situation could be worse in secondary schools where personnel with baseline computing skills are only concerned with the use of CISs regardless of the perennial security risks associated with these information systems assets. In light of this, secondary schools need assistance from within or outside to initiate and guide them in performing risk management for their CIS.

Some risk management techniques are either too difficult to be understood or to be used by small-scale organisations, subsequently these organisations resort to unendorsed methods or avoid carrying out risk management exercises completely (Alberts & Dorofee, 2001; Beachboard *et al*. 2008). To encourage secondary schools to perform risk management, a simple and participatory risk management method in the qualitative category namely, OCTAVE should be used. Unlike other risk management methods which focus much on technical risks, OCTAVE deals with organisational risk in addition to technical risks (Ganthan *et al*. 2009).

1.2.4. Overview of the OCTAVE-small risk management method

Secondary schools require risk management methods that enable managers and users to be acquainted with their information systems security issues so that they can improve their information security posture without relying much on outside experts. The OCTAVE method has been identified as the most appropriate method for this purpose because it is a process-driven method which identifies, prioritises and manages information security risks within an organisation's information system (Alberts & Dorofee, 2004; Panda, 2009). OCTAVE is designed to provide complete information about information security risk management for a given organisation (Alberts & Dorofee, 2002). The OCTAVE risk management process is self-directed because it encourages people from within the same organisation to collaboratively assume the responsibility of setting the organisation's security strategy (Panda, 2009; Tiwari, 2010), an outcome this study attempts to achieve.

Variations of the OCTAVE method offer an organisation a choice of risk management techniques suitable to that organisation depending on the size and layering of its information systems (Panda, 2009). Secondary schools have a flat-layered hierarchical structure, therefore, their information systems could be assessed and analysed using OCTAVE for small-scale organisations (OCTAVE-small) risk management method. Alberts and Dorofee (2002) and (Sosonkin, 2005) argue that by implementing OCTAVE-small risk management process, an organisation tends to benefit from the catalogue of practices, threat profile and catalogue of vulnerabilities. These catalogues can act as references for secondary schools which decide to embark on information security risk management exercises using personnel with baseline computing skills.

This study capitalises on the flexibility of OCTAVE-small which can be customised to suit secondary schools' unique information systems risk environments, security, objectives and the level of skills available. The customised OCTAVE-small method to be used in this study will be based on four processes unlike the conventional three-phased OCTAVE-small. This is intended to make the risk management exercise user friendly and interesting to the school personnel and at the same time achieving research objectives. OCTAVE-small is discussed in detail in Chapter 6.

1.3. RESEARCH CONTEXT

Schools in Vhembe District have computerised records management systems that form the core of their information systems. These information systems are supported by local area networks (LANs). Normally the LANs are connected to the Internet to provide access to the web. Personnel with baseline computing skills and knowledge administer these CISs. Educators and learners access these facilities, especially when browsing the web and accessing e-learning materials or entering marks on the databases. Administrative computers holding vital school information are also part of these LANs. There is a high likelihood that critical information in secondary schools is exposed to risks from these internal users and/or unknown external intruders.

Under these circumstances, schools are most likely to find it difficult to secure their information systems against multiple threats they could be exposed to. Risk assessment and analysis are critical activities in identifying information assets, the risks to those assets and procedures to mitigate the risks to the assets (Marchany, 2003). Due to lack of expertise in risk management in schools, the possibility of conducting risk management exercise is remote. This means that school management and users would remain ignorant of the risks to which their information systems are exposed to.

1.4. MOTIVATION FOR THIS STUDY

This study was motivated by the following observed factors:

- The proliferation of CISs in secondary schools may have implications for information security in these organisations. There could be a high prevalence of information security breaches in schools that management and users are not aware of. These breaches could compromise information confidentiality, integrity and availability in secondary schools CISs and need to be identified and mitigated.

- The Internet has become part of the information systems in schools and there is clear evidence that organisations can operate effectively by capitalising the efficiency and communications capabilities provided by the Internet (Wack, Tracy & Souppaya, 2003; Steve, 2007; Al Saif, 2009). At the same time, the Internet has become one of the biggest potential sources of threats that may put an organisation's information system at risk due to multiple information security breaches by intruder attacks and malware infections (Wack *et al*. 2003; Al Saif, 2009). Unauthorised users capitalise on unsecured networks to gain access to the Internet or other vital information systems without being detected. The majority of schools that use CISs may hardly have the capabilities of detecting security violations of this nature.

- An upsurge in the number of computer users with different motives, translates to an increase in information security risk in secondary schools. For example, Park, Min, Lee, Lee and Lee (2006) emphasise that a large proportion of reported information security breaches within an organisation are due to computer users' intentionally and unintentionally motives. In secondary schools, the extent to which these users contribute to information security breaches intentionally or accidentally deserves research attention.

The cited factors are indicators that as secondary schools thrive on CISs they also need to conduct information security risk management exercises to ascertain their CISs security status.

1.5. THE PROBLEM STATEMENT

Secondary schools hardly have any information security personnel to help them perform risk management exercises and to secure their critical CISs assets against risks they are exposed to. If this situation persists unabated, these CISs face disastrous consequences that could subsequently lead to their inevitable collapse. Therefore, to sustain the continued use of CISs in secondary schools, there is a dire need to educate school managers and CISs users on how to conduct risk management exercises and also to recommend implementable risk mitigation strategies. This research focuses on information security risk management in secondary schools' CISs implementing the Operationally Critical Threats, Assets and Vulnerability Evaluation for small-scale organisations (OCTAVE-small) risk management method.

1.6. RESEARCH OBJECTIVES

This study was guided by one main research objective and three sub-objectives stated below.

1.6.1. Main research objective

The main objective of this research study was to assist secondary schools that used CISs to develop a set of guidelines they would use to effectively manage information security risks in their computerised information systems.

1.6.2. Sub-objectives

The research sub-objectives were:

1. *To systematically gather data on critical assets and information security controls in CISs in secondary schools;*

   This sub-objective is explored in chapters 3,4, 6, 7 and 8 of this study.
2. *To identify an easy to use risk management methodology that non-technical personnel in secondary schools can utilise.*

   A number of subsections in chapters 4, 5, 6 and 7 have been dedicated to the risk management process from a theoretical and a practical standpoint. It is in Chapter 7 that this study performs the risk assessment and analysis on data collected from various sources.
3. *To deduce generic guidelines that could be followed during information security risk management at a secondary school that take into account CISs users who are not experts in risk management.*

   Conventional mitigation strategies are discussed in Chapter 4. In chapters 7 and 8, the study proposes a number of simple protection and mitigation strategies for implementation at secondary school level.

1.7. ASSUMPTIONS, DELINEATIONS AND LIMITATIONS

An overview of research assumptions, delineations and limitations is outlined below.

1.7.1. Assumptions

This study assumes that

- school managers and users of CISs would voluntarily participate and cooperate by providing the researcher with all vital information needed for the success of this study;
- participants would be familiar with the research instruments to be used in this study; and
- the participants' perspectives would be meaningful, knowable and be made explicit that they affect the success of this study positively.

1.7.2. Delineations

This research focused mainly on information security risk management for CISs in selected secondary schools. Any other forms of risks to the school information systems outside computerisation were not investigated. Only the OCTAVE-small risk management method was used in this study. Population samples were drawn from the current regular users of CISs. Only secondary schools took part in this research study.

1.7.3. Limitations of the study

There are a number of factors over which the researcher has no control and which may affect the outcome of this research. The following factors are considered as limitations to this study:

- environment, behaviour or event of interest could be inaccessible and observation simply becomes impossible or difficult (Foster, 2006). Accessibility to CISs and users may be restricted by school management for their own reasons;
- the presence of an outsider in the school could be regarded as an intrusion and cause the observed sample members to behave otherwise. This may cause the account of observed behaviour to be an inaccurate representation of how the subjects behave naturally (Ritchie & Lewis, 2005);
- time allocated to the researcher to collect data in schools may be insufficient. Schools may limit the time the researcher takes for collecting data at a particular instance; and
- school management may also interfere with data collection processes as they redeploy resources as per demand.

1.8. RESEARCH METHODOLOGY AND DESIGN

This section examines research and methodology design for this research study.

1.8.1. Research methodology and design

A research methodology is a strategy of inquiry which moves from the underlying philosophical assumptions to research design and data collection (Myers, 2004). Research design and data collection techniques depend on the research methodology adopted for a particular problem. Choosing the most appropriate research method from multiple methods is a difficult task (Ritchie & Lewis, 2005; Foster, 2006; Babbie, 2007; Denzin & Lincolin, 2008). The choice of a research method is subject to the nature of the research problem, or the social phenomena to be explored (Noor, 2008)**.** This study uses a qualitative case study research strategy, an in-depth examination of a single or more related instance(s) of some social phenomenon such as a village or family (Myers, 2004; Babbie, 2007; Gray, 2009). Information security risk management in schools is a social issue because it has a direct or indirect effect on how schools with CISs conduct their everyday business and how the inherent risks are likely to affect the society.

Currently, research interests in information systems have shifted from technical to organisational issues (Myers, 2004), making the case study research strategy particularly well-suited for information security risk management in secondary schools. Additionally, a case study is a naturalistic and interpretive method concerned with understanding the meaning with which people attach to actions, decisions and values within their social worlds (Denzin & Lincolin, 2008).

The OCTAVE-small risk management method will be used in two secondary schools in Thohoyandou Cluster of the Vhembe District. Risk assessment and analysis was conducted in terms of physical, human, malicious and natural disaster threat sources on the CISs of those selected schools.

1.8.2. Population and sampling procedures

A population is a group of individuals who have the same characteristics (Cresswell, 2005). The population for this research would be consisted of those individuals who use CISs in secondary schools. Ritchie & Lewis (2005) recommend the use of non-probability sampling method for selecting the population samples for a qualitative research. Non-probability sampling allows the researcher to select individuals and sites because they are available, convenient, and represent some characteristics the researcher wants to study (Cresswell, 2005; Leech & Onwuegbusie, 2007). In a secondary school setup, the main users of CISs were office educators who had more-or-less similar computing skills and knowledge. The samples were drawn using purposive sampling strategy, a non-probability sampling method in which the units to be observed were selected on the basis of the researcher's judgement on which ones were the most useful or representative (Creswell, 2005; Babbie, 2007). This study collected data, presented and analysed it as outlined in subsection 1.8.3 below.

1.8.3. Data collection, analysis and presentation

This section outlines data collection, presentation and analysis which were important aspects of this study.

1.8.3.1.Data collection

Data collection involves applying the instruments to the sample or cases selected for the investigation (Merriam, 2009; Mouton, 2009). Studies in qualitative research indicate that most of the qualitative data are non-numeric (Myers, 2004). Consequently, qualitative research relies on data collected from a small number of individuals or sites (Myers, 2004), through interviews, observational, fieldwork and archival research techniques (Tere, 2006; Denzin & Lincolin, 2008).

In this case study, data were gathered using observation checklists, inspection checklists and interview schedules. Effectively, these techniques allowed close contact between the researcher and the research participants, making them interactive and developmental, simultaneously allowing emergent issues in computerised information security to be explored deeper (Creswell, 2005; Ritchie & Lewis, 2005). Semi-structured interviews and participatory observation were the main data collection techniques for this research**.**

1.8.3.2. Presentation of data and reporting on findings

Results from this research are presented on tables and reports. Reporting of findings is done through narrative and descriptive discussions. These summarise the findings from the data analyses with respect to each sub-objective.

1.8.3.3. Data analysis

In this study, audiotaped interviews were transcribed and then analysed using qualitative description with constant comparison and inductive data analysis technique. This also applied to textual data from interviews and notes from participatory observation which were analysed using a qualitative techniques as recommended by Cresswell (2005) and Werlinger, Hawkey, Botta, & Beznosov (2009).

1.9. RESEARCH ETHICS

Conducting a research with human beings as subjects brings forth ethical issues that have to be addressed from the onset (Ritchie & Lewis, 2005; Marshall & Rossman, 2006; Babbie, 2007). Research ethics refer to moral principles guiding the researcher to conduct a research in a way that goes beyond adopting the most appropriate research methodology, but conducting a research in a responsible and morally defensible manner (Gray, 2009). The ethical issues this research study took into account were consent of individual participants, protection of identity through practising anonymity and confidentiality of participants, protection of participants and other researchers from harm, and avoiding the use of deception (Ritchie & Lewis, 2005; Babbie, 2007; Gray, 2009). Furthermore, the researcher abided by the requirements of the citation of other researchers' work and reporting accurate results and research findings. Written permission to conduct research with different subjects in selected schools was granted by the relevant education authorities. The participants were adults from selected schools and their consent was sought well before hand.

1.10. RESEARCH CONTRIBUTION

This research seeks to underpin the process of information security risk management in CISs in South African secondary schools. The research study provides a set of guidelines that secondary schools would possibly utilise to manage information security risks in their CISs. The study would also strive to support and promote active participation in risk management by users with baseline information technology skills using generic protection and mitigation strategies improvised by schools. Instead of over-relying on large organisations for risk management, schools would be able to improvise information security solutions peculiar to their own computing environments. Therefore, the set of risk management guidelines deduced in this study might be expanded and adopted by primary and secondary schools that use CISs across South Africa.

1.11. RESEARCH PLAN

The purpose of a research plan is to guide the researcher in completing set tasks in a given time frame. The research plan for this study is depicted on Table 1.1 below.

Table 1.1: Research Action Plan

Research Activity	**Date of completion**
Final Research Proposal	3 October 2011
Chapter 2: Research methodology	01 March 2012
Chapter 3: Information security overview	01 June 2012
Chapter 4: Risk management process	02 July 2012
Chapter 5: Risk management methodologies	30 August 2012
Chapter 6: The OCTAVE method	30 October 2012
Chapter 7: Data Collection, presentation, analysis and interpretation	
Designing Instruments and pilot study	30 November 2012
Data collection, analysis and interpreting results	30 May 2013
Chapter 8: conclusion	30 August 2013
First final draft	30 September 2013
Second final draft	30 October 2013
Third final draft	15 November 2013
Submission	February 2014

1.12. PUBLICATIONS

The following peer-reviewed publication was derived from this research study. It was published and presented at an International Conference Information Security for South Africa 2013 where valuable feedback and comments were attained and incorporated in this study. Moses Moyo, Hanifa Abdullah and Rita Nienaber, 2013, **Information Security Risk Management in Small-scale organisations: A Case Study of Secondary Schools' CISs**. In Proceedings of 2013 Information Security for South Africa, (ISSA 2013, #70) IEEE Catalog Number, CFP13661-CDR, ISBN 978-1-4799-0809-7 (14 - 16 August 2013).

The research paper was presented at ISSA conference on the 14th of August 2013. The Abstract of this paper was also presented at the South African Institute for Computer Scientists and Information Technologists (SAICSIT) Masters and Doctoral Symposium on the 1st of October 2012. The researcher has an additional publication. Moyo, M and Abdullah, H. 2013. **Enhancing and Enriching Students Reading Experience by using Social Media Technologies**, Mousaion South African Journal of Information Studies 31 (2) 2013, page 135 – 56, ISSN 0027-2639

1.13. DEFINITION OF KEY TERMS

This study uses a number of terms or concepts that readers may be familiar or unfamiliar with. Some of the terms have different meanings from those they denote in this study. This subsection is dedicated to definitions of key terms used in this study.

Computerised information system: This is a computer-based information system that processes data into information useful in the support operations of an organisation and decision making by management.

Information security risk analysis: information security risk analysis is a multi-step process of determining exposure to security threats that an organisation faces (Goel & Chen, 2008).

Information security risk: Information security risk is any possible threat that exploits vulnerability in an information asset of an organisation to cause disruption to the organisational routines and processes in one way or the other (Tiwari, 2010).

Information security: Information security is the practice of ensuring that information is only read, heard, changed, broadcast and otherwise used by people who have the right to do so (Kite, 2009). It is the preservation of confidentiality, integrity and availability of information (Theoharidou *et al*. 2005)

Information system asset: Information system asset refers to any company-owned information system or hardware that is used in the course of business activities (Rouse, 2007). An information system asset is anything of value that an organisation needs to accomplish its mission (Ciechanowicz, 1997).

Information system: Information system is the collection of technical and human resources that provide the storage, computing, distribution, and communication for the information required by all or any part of an organisation (Rouse, 2008).

Risk assessment: Hoo (2000) regards risk assessment as the process of identifying, characterizing, and understanding risk; that is, studying, analysing, and describing the set of outcomes and likelihoods for a given endeavour.

Risk management: Risk management process is defined as a systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk (AS/NZS ISO 31000:2009, 2009).

Risk mitigation: The process by which an organisation introduces specific measures to minimise or eliminate unacceptable risks associated with its operations (Goel & Chen, 2008).

Risk: A risk is the potential for an unwanted event to occur and is a function of the likelihood of that unwanted event occurring and its consequences (Siu, 2007). A risk can be an event, occurrence or actions that may prevent an organisation from realising its ambitions, plans and goals (Alhawari, Karadsheh, Talet & Mansour, 2012).

Security control: A security control is an action, process, device, or system that can prevent, or mitigate the effects of, threats to a computer, server or network (Meier, Mackman, Dunner, Vasireddy, Escamilla & Murukan, 2006). The process by which an organisation introduces specific measures to minimise or eliminate unacceptable risks associated with its operations.

Small-scale organisation: A small organisation is a privately owned or government organisation with full time employees between ten and eighty people.

Threats: A threat is a natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property (Elky, 2006; Metras, 2008)

Virus: A virus is a computer program designed to disrupt computer operations by replicating and inserting its copies into other computer programs, data files, or the boot sector of the hard drive.

Vulnerability: Vulnerability is a combination of the attractiveness of a facility as a target and the level of deterrence and (or) defence provided by the existing security controls (Renfroe & Smith, 2011). Vulnerability is the degree to which the exposed elements of an information system will suffer a loss from the impact of a hazard.

Worm: This is an independent program which replicates from computer to computer across the network connections and always clogging networks and information systems as it spreads.

1.14. STRUCTURE OF THE DISSERTATION

This dissertation is organised into eight chapters grouped into four parts, I, II, III and IV. Each chapter discusses important aspects of the research study. The outline of the research is given below and diagrammatically depicted on Figure 1.1.

PART I: INTRODUCTION

This section consists of chapters 1 and 2, the introduction and the research methodology respectively.

Chapter 1: Introduction

This chapter introduces the research and places it into perspective by addressing key aspects namely research background, context, motivation, statement of the problem, objectives, assumptions, delimitations, limitations and research ethics. The chapter also gives the outline of the research

Chapter 2: Research methodology

This chapter discusses the methodology, research strategy, design, data collection and analysis techniques and tools. The case study research methodology has been discussed from both theoretical and practical views. This chapter also justifies qualitative research methodology, strategy, design and data collection techniques and analysis.

PART II: LITERATURE REVIEW

This section comprises of Chapter 3, 4 and 5. Each chapter deals with a specific and important topic which contributes to the overall outcome of this research study.

Chapter 3: Information Security Risks Overview

This chapter is on information security and key concepts vital to this research study. The need to maintain or reduce risks in CISs is tied to the major goals of information security namely, confidentiality, integrity and availability. The chapter demonstrates the link between various information security concepts: assets, risk, threats, vulnerabilities, exposures, controls and risk management.

Chapter 4: Risk management process

Chapter 4 is a detailed examination of scholarly work focusing on information security risk management. Attention is given to risk management process and its components; risk assessment, analysis, and mitigation as exemplified AS/NZS ISO 31000:2009 risk management framework.

Chapter 5: Risk management methodologies

Chapter 5 discusses quantitative and qualitative risk management methodologies. Merits and demerits of each category of methods are also discussed in detail in order to justify the use of a qualitative risk management method namely, OCTAVE-small.

PART III: EMPIRICAL STUDY

This section discusses OCTAVE-small risk management and demonstrates how it will be used in this research study. The discussions are linked with those made in Section I particularly Chapter 2, Research Methodology. Data are presented, analysed and interpreted qualitatively.

Chapter 6: The OCTAVE-small methodology

This chapter deals with the practical aspects of data collection in schools. It describes how the OCTAVE method will be used in conjunction with the research tools discussed in Chapter 2.

Chapter 7: Data presentation, analysis and interpretation

A rigorous analysis of data is carried out using narrations and constant comparison methods. Trends and themes are identified and discussed. Results are presented following each data analysis technique.

PART IV: CONCLUSION

In this section, the findings are stated, discussed and conclusions made. Reflections and recommendations for further research are put forward.

Chapter 8: Contribution and Conclusion

This chapter discusses research findings and then state conclusions from these findings. The researcher reflects on the research contribution and gives recommendations for further studies.

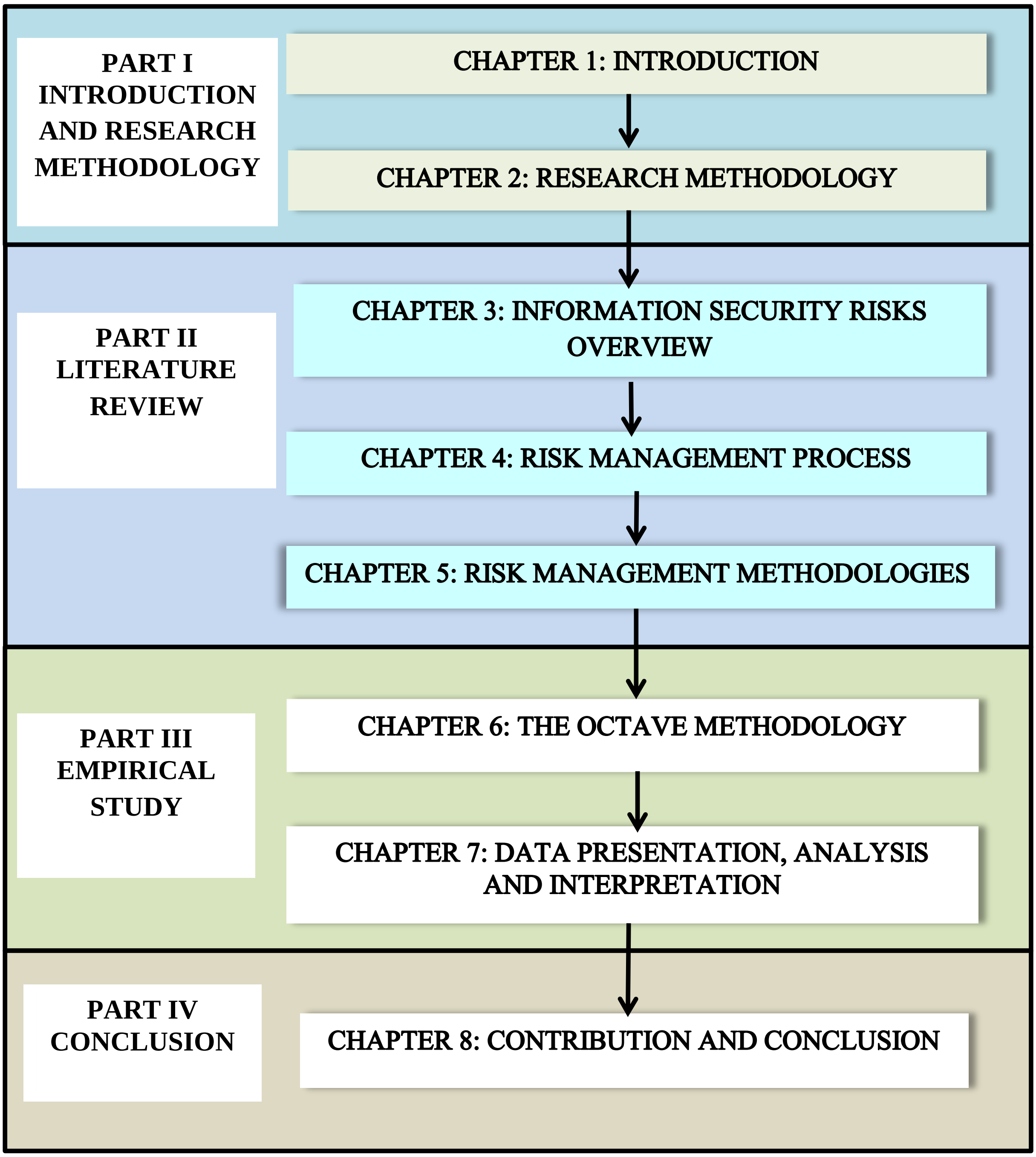

PART I
INTRODUCTION AND RESEARCH METHODOLOGY
CHAPTER 1: INTRODUCTION
CHAPTER 2: RESEARCH METHODOLOGY
PART II
LITERATURE REVIEW
CHAPTER 3: INFORMATION SECURITY RISKS OVERVIEW
CHAPTER 4: RISK MANAGEMENT PROCESS
CHAPTER 5: RISK MANAGEMENT METHODOLOGIES
PART III
EMPIRICAL STUDY
CHAPTER 6: THE OCTAVE METHODOLOGY
CHAPTER 7: DATA PRESENTATION, ANALYSIS AND INTERPRETATION
PART IV
CONCLUSION
CHAPTER 8: CONTRIBUTION AND CONCLUSION

Figure 1.1: Outline of research chapters

1.15. CONCLUSION

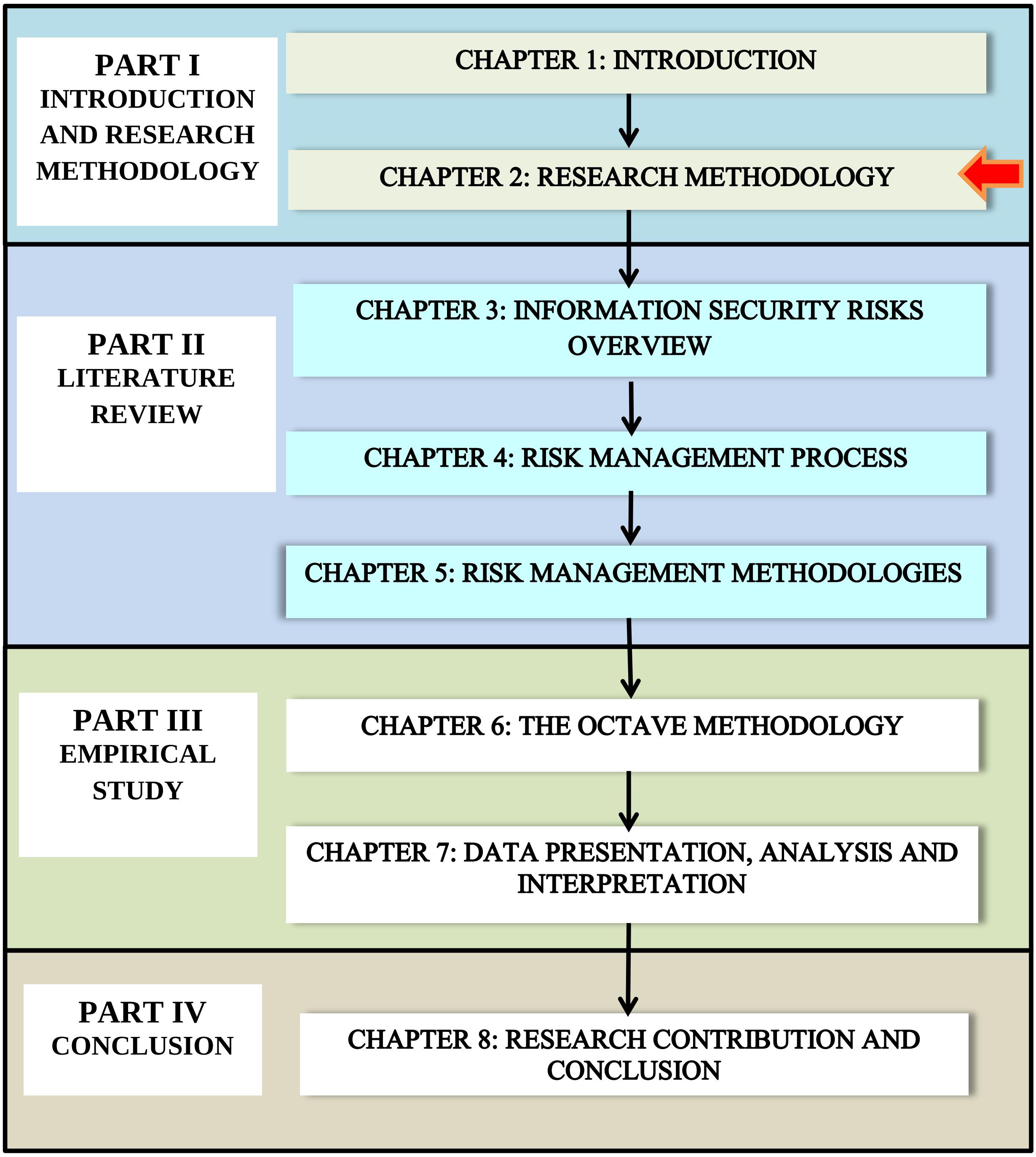
Schools as emerging users of CISs should play a key role in information security within and outside their premises. This chapter has highlighted the need to conduct information security risk management exercises in secondary schools' CISs. The chapter introduced the problem of information security risks that secondary schools may be experiencing. The research is intended to educate school managers and CISs users in conducting simple risk management programmes on their own. To achieve this, a qualitative case study would be carried out in two selected secondary schools in which the OCTAVE-small method would be implemented. The chapter further discussed the motivation, context and problem statement of this study. Research objectives were also stated in order to guide the research study. Preliminary literature review on issues in information security risks and risk management is also documented. Data collection techniques have been identified as participatory observation, physical inspections and interviews. Purposive sampling would be used to select secondary schools and also the subjects of this research. The structure of the dissertation is also outlined and depicted diagrammatically in Figure 1.1.

This study is an initiative to enlighten school managers and CISs users on information security risk management. It is anticipated that the findings of this study will play a crucial role in information security risk management in South African schools and could assist these organisations in performing risk management exercises in their CISs on regular bases.

The next chapter, Chapter 2 discusses research methodology, a crucial component of this study. It also discusses the research strategy, methods and data collection tools. It also justifies the selection of the qualitative case study.

CHAPTER 2

2. RESEARCH METHODOLOGY


PART I
INTRODUCTION AND RESEARCH METHODOLOGY
CHAPTER 1: INTRODUCTION
CHAPTER 2: RESEARCH METHODOLOGY
PART II
LITERATURE REVIEW
CHAPTER 3: INFORMATION SECURITY RISKS OVERVIEW
CHAPTER 4: RISK MANAGEMENT PROCESS
CHAPTER 5: RISK MANAGEMENT METHODOLOGIES
PART III
EMPIRICAL STUDY
CHAPTER 6: THE OCTAVE METHODOLOGY
CHAPTER 7: DATA PRESENTATION, ANALYSIS AND INTERPRETATION
PART IV
CONCLUSION
CHAPTER 8: RESEARCH CONTRIBUTION AND CONCLUSION

2.1. INTRODUCTION

Research in any given field of study utilises research methodologies, models and strategies based on different philosophical foundations and forms of reality. These philosophical assumptions play a crucial role in making a researcher and readers understand the overall perspective from which the study is designed and carried out (Krauss, 2005).

Chapter 2 delineates the research methodology followed in this dissertation and also explores some contextual factors that affect and influence the choice of a research methodology. The chapter justifies the use of the qualitative research methodology that implements an interpretive case study strategy in which data generating methods are participatory observation, physical inspection and interview. Research instruments to be constructed and used in this study are also introduced. This study intends to implement the research process suggested by Oates (2006), shown in Figure 2.1.

This chapter's structure consists of a brief introduction, a detailed discussion of the research methodology under different subsections, namely choosing a research methodology, qualitative research methodology, criteria for qualitative research methodology, research paradigm and data analysis method. The scope of the study and conclusion are also presented as the penultimate and ultimate sections of the chapter.

2.2. RESEARCH METHODOLOGY

The purpose of this research study was to assist secondary schools that used CISs to develop a set of guidelines they would use to effectively manage information security risks in their computerised information systems. This study was also intended to enlighten secondary school management and users on the essence of information security. The research study was performed in two selected secondary schools in Thohoyandou Cluster, Vhembe District. The Operationally Critical Threat, Asset and Vulnerability Evaluation for small-scale organisations risk assessment and analysis method was used to study CISs in the sampled secondary schools. For this research study to be successful, it utilised an information systems research process suggested by Oates (2006) depicted diagrammatically in Figure 2.1.

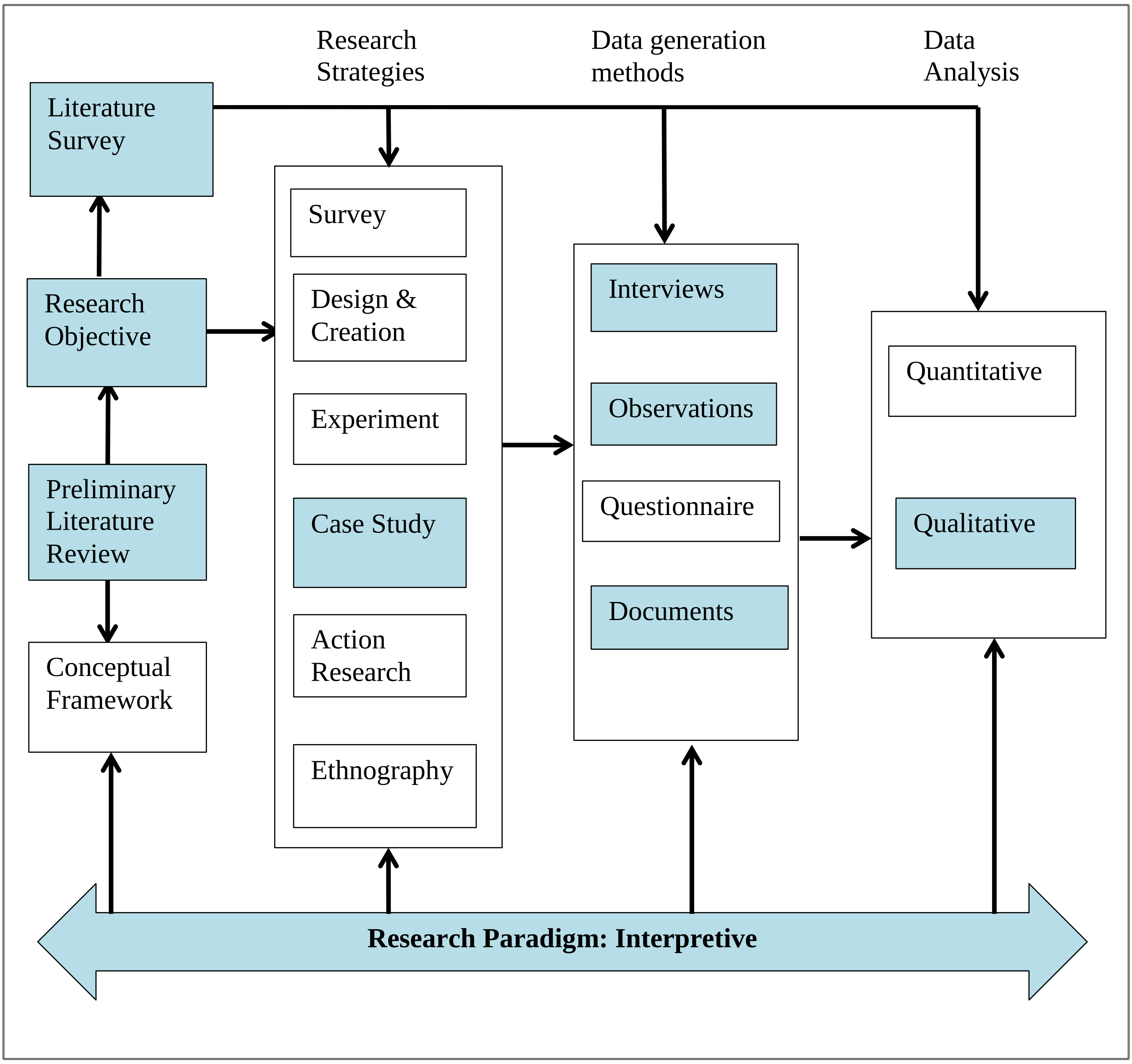


Figure 2.1: The research methodology model

Source: Oates (2006) and Nienaber (2008)

At this stage, the research route is indicated by shaded components of this diagram.

2.2.1. Choosing a research methodology

This research study utilised a case study research strategy based on qualitative data analysis techniques. The choice of a research methodology was determined by the research problem being dealt with; in this case, the information security risk management in secondary schools' CISs. This decision was based on the recommendations by a number of research studies that emphasise the importance of selecting a research methodology by first looking at the phenomenon being researched (Cavaye, 1996; Krauss, 2005; Noor, 2008; Mouton, 2009). These authors suggest that the research methodology employed in a research study should focus on a particular phenomenon of interest. Instead of being committed to a particular paradigm, the determining factor should be focusing on what the researcher is attempting to achieve (Cavaye, 1996; Mouton 2009). Echoing the same sentiments, Noor (2008) argues that the choice of a research methodology depends on both the nature of the research problem or the social phenomena being explored and the research environment in which this takes place. The argument is that focusing on the social problem being studied rather than the methodology, enables a researcher to select a more appropriate methodology for an inquiry (Falconer & Mackay, 1999).

In an attempt to assist secondary schools to perform risk management exercises for their CISs, this research study adopted a research methodology that enabled data collection from these sites while the information systems assets were in use. The researcher gathered data from the information systems assets, the users and the environment in which they were being used. The research methodology used in this study was intended to provide the researcher with an opportunity to collect data in the natural settings of the systems, and then interpret it according to the meanings the users attached to these data. The qualitative research methodology was found to be suitable, especially in the interpretive paradigm. The basis on which the qualitative research methodology was chosen is discussed in subsequent subsections.

2.2.2. Qualitative research methodology overview

A number of authors such as Myers and Avison (2002), Goldkuhl (2012) and Myers (2011) encourage the use of a qualitative methodology when the research study attempts to understand or promote knowledge construction through social meanings attached to human experiences. In this study, the use of a qualitative research methodology in information security risk management with non-technical personnel in schools provides the researcher with an opportunity to understand the risks associated with these information systems from the users' point of view and related empirical evidence. The research strategy and methods used in this study lead to the understanding of the context of information systems in secondary schools and how the risks affect the context in which these information assets are used.

Qualitative research is an inquiry process of understanding a social or human problem based on building a complex, holistic picture, formed with words, reporting detailed views of informants, and conducted in a natural setting (Cresswell, 2005). A qualitative research methodology involves an interpretive and naturalistic approach to its subject matter in which researchers study things in their natural settings, attempting to make sense of or interpret phenomena in terms of the meanings people bring to them (Denzin & Lincolin, 2008). The primary goal of a qualitative research approach is to describe and then understand as opposed to mere explaining social action (Babbie & Mouton, 2001). This presents the researcher with an opportunity to understand the meaning that people continually construct about an identified problem (Merriam, 2009), in this case how users of information systems make sense of security risks and their experience in information systems. Therefore, the purpose of qualitative research methodology in this research study is to adopt, create and use a variety of qualitative research methods to describe the rich interpersonal, social and cultural contexts in which CISs are used in secondary schools.

2.2.3. Criteria for qualitative research

Two domains need to be considered when developing a qualitative research design: the criteria for soundness and demonstrating that the proposed work would be useful to the research context and the initial research objectives or questions (Marshall & Rossmann, 2006; Trochim, 2006). The criteria for soundness (objectivity) of qualitative research are related to, but defined very differently from those used in the quantitative research tradition (Golafshani, 2003; Trochim, 2006). The four main criteria for objectivity namely credibility, transferability, dependability and conformability as applied to qualitative research are described by Babbie and Mouton (2001), Marshall and Rossmann (2006) and Trochim (2006). Table 2.1 is an illustration of quantitative and qualitative notions of objectivity propounded by Babbie and Mouton (2001) and Trochim (2006).

Table 2.1: Quantitative and qualitative views of objectivity

Traditional criteria for judging quantitative research	**Traditional criteria for judging qualitative research**
Internal validity	Credibility, trustworthiness
External validity	Transferability
Reliability	Dependability
Objectivity	Conformability

Source: Babbie and Mouton (2001) and Trochim (2006)

A brief discussion of each qualitative notion of objectivity is given below.

2.2.3.1. Credibility

Qualitative studies use a number of terms such as quality, rigour, credibility and trustworthiness to describe research methodology validity (Golafshani, 2003). Credibility means accurate identification and description of the phenomenon by the research study (Yin 2003). This involves determining if the results of qualitative research are credible or believable from the perspective of the participants in the research (Trochim, 2006). The strength of a qualitative research study that seeks to explore a problem or process depends on its credibility (Marshall & Rossmann, 2006; Yin, 2003). Research credibility is ensured by clearly stating the parameters of the study such as the settings, population and theoretical framework (Trochim, 2006). In this research, credibility deals with the quality of data collected and the soundness of reasoning that lead to the conclusions based on the data. This study preserves credibility through a number of strategies namely:

- a proper balance between the researcher's involvement in the research, influence on other participants and its effects on the data to be collected (Morse, Barrett, Mayan, Olson & Spiers, 2002);
- the researcher avoiding preconceived ideas about the subject being studied during data analysis, but to concentrate on the empirical data gathered during the research (Golafshani, 2003);
- providing justification in the event that the researcher develops alternative explanations and finding (Voss, Tsikriktsis & Frohlich, 2002); and
- triangulation, the use of multiple data generating methods, for the researcher to consider observed phenomena from different perspectives (Cresswell and Miller, 2000).

2.2.3.2. Transferability

Transferability refers to the degree to which the results of qualitative research can be generalised or transferred to other contexts or settings that may be problematic (Marshall & Rossmann, 2001; Dooley, 2002; Trochim, 2006). Research transferability is enhanced by thoroughly describing the research context and the assumptions that are central to the research (Marshall & Rossmann, 2001; Dooley, 2002). It is the responsibility of the researcher or person who wishes to transfer the results to a different context to make the judgment of how sensible the transfer would be (Trochim, 2006). This study uses a multi-case or collective of cases to cater for transferability.

2.2.3.3. Dependability

Dependability is the ability of a research study to account for the ever-changing context within which the research occurs (Trochim, 2006). While quantitative approaches view reliability as based on the assumption of replicability or repeatability, qualitative approaches emphasise on dependability instead (Voss *et al*. 2002). A qualitative research is difficult to replicate, therefore, the need to emphasise on transparency and explicitness about the research processes to be conducted and justification of the choices of research methods and data collection tools (Golafshani, 2003). To achieve this, Yin (2003) and Trochim (2006) encourage the researcher to take responsibility in describing the changes that occur in the setting and how these changes would affect the way the researcher approached the study. For this research, measures for maintaining dependability involve systematically gathering data by means of prior identified key items in information systems users' activities and observable information security risks in the schools involved. This would extend to the processing of data using consistent coding systems and verifiable descriptions and interpretations.

2.2.3.4. Conformability

Conformability is the degree of neutrality or the extent to which the findings of a study are shaped by the respondents and not by the researcher's bias, motivation or interest (Lincoln & Guba, 1985), or the degree to which the findings of a research study could be confirmed or corroborated by others (Trochim, 2006). This means that the focus of the study should be evidence itself and not some inherent characteristics of the researcher (Marshall & Rossmann, 2006; Yin, 2003). Research conformability can be achieved by documenting all the procedures for checking and rechecking the data throughout the study (Trochim, 2006). This allows the researcher to conduct and examine the data collection and analysis procedures and make judgements about the potential for bias or distortion (Golafshani, 2003; Yin, 2003; Trochim, 2006). Alternatively, the researcher can make the data available for scrutiny by research participants and other interested readers (Golafshani, 2003). In this research study, participants will have access to all data collected so that they confirm the credibility of the data.

2.2.4. Research paradigm

A research paradigm is an all-encompassing principles system of interrelated practice and thinking that define the nature of enquiry along these three dimensions (TerreBlanche & Durrheim, 1999). A paradigm is a pattern, model or shared way of thinking (Bharadwaj, 2000; Myers, 2004; Oates, 2006). Different philosophical paradigms hold different views on the nature of reality about the world (ontology) and the methods used to acquire knowledge about it (epistemology) (Nienaber, 2008; Myers, 2011). Each paradigm is implemented using related methodological approaches and strategies (Nienaber, 2008). Research in information systems is based on three main paradigms namely positivist, interpretive and critical (Bharadwaj, 2000; Myers, 2011). Existing literature on information systems research methodologies indicates that positivist and interpretive paradigms are the two major competing philosophical perspectives in use in this area (Myers, 2004). The same literature also reports that qualitative research is mainly influenced by interpretive philosophical perspective (Bharadwaj, 2000; Myers & Avison, 2002; Weber, 2004; de Villers, 2005; Stockdale & Standing; 2006). Based on the research problem to be explored by this study, the interpretive paradigm has been identified as the most suitable philosophical assumption.

Research studies that utilise interpretive paradigm emphasise the understanding of phenomena through the meanings that people assign to them (Myers, 2004; Warden & Wong, 2007). An interpretive researcher seeks to understand values, beliefs and meanings of social phenomena in order to gain a deep and sympathetic understanding of human cultural activities and experiences (Kim, 2003; Myers, 2004). This implies that, interpretive methods of research in information systems are designed to produce an understanding of the context of the information system, and the process whereby the information system influences and is influenced by that context (Walsham, 2006; Nyame-Asiamah & Patel, 2009). The interpretive perspective emphasises the creativity aspects of science and how scientific knowledge is built through subjective interpretations of observations in the context of the researcher's knowledge and mental models (Bharadwaj, 2000; Goldkuhl, 2008; Myers, 2009).

2.2.5. Preliminary literature review

After identifying the research methodology, this study embarks on a preliminary literature review in the field of study in which the problem falls. This exercise is meant to ascertain the extent to which this problem has been addressed by previous researchers and also the gaps and outstanding issues to be addressed. This preliminary literature review helps in formulating research objectives for the study. Figure 2.1 shows the research process being followed in this study.

2.2.6. Objectives

This study was guided by objectives. The main objective and its sub-objectives are revisited below.

2.2.6.1. Main objective

The main objective of this research study was to assist secondary schools that used CISs to develop a set of guidelines they would use to effectively manage information security risks in their computerised information systems.

2.2.6.2. Sub-objectives

The research sub-objectives were to:

1. *systematically gather data on critical assets and information security controls in CISs of two secondary schools;*
2. *identify an easy to use risk management methodology that non-technical personnel in secondary schools can utilise.*
3. *deduce generic guidelines that could be followed during information security risk management at a secondary school that take into account CISs users who are not experts in risk management.*

Having identified the research approach, paradigm and objectives for this study, it is important to discuss the research strategy to be used. In the following subsection, the researcher discusses the case study research strategy which is used in this study.

2.2.7. Case study research strategy

The development of a research strategy is based on the research paradigm that the research study adopts (Merriam, 2009). A research strategy is a set of guidelines and instructions to be followed in addressing a research problem (Mutchnick & Berg, 1996). The main function of a research strategy is to enable the researcher to maximise the credibility of the eventual results (Mouton, 2009). Commonly used research strategies are the survey, design and creation, experiment, case study, action research and ethnography (Oates, 2006), shown on Figure 2.1. This research study utilises a qualitative case study research strategy. A case study is:

- an empirical inquiry that investigates a new phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident (Yin, 2003).
- a research strategy used to generate an in-depth, multi-faceted understanding of a complex issue in its real-life context (Crowe, Cresswell, Robertson, Huby, Avery and Sheikh, 2011).

Therefore, a case study is a practical-based research strategy in which a researcher studies contemporary issues in their natural settings with the intention of gaining an understanding of the complexities surrounding them.

A case study can be used to study a single or a multiple of related cases of some social phenomenon such as a village or family (Babbie, 2007; Gray, 2009). This can also extend to schools which are social entities. There are three reasons that make a case study the most viable research strategy one could use in trying to solve a social problem. These include:

- the opportunity for the researcher to study the phenomenon in its **natural settings** with the intention of understanding the nature of current processes in an area which has been barely studied previously (Shanks & Parr, 2003; Yin, 2003; Myers, 2011);

- the opportunity for the researcher to ask the **‘what, how and why’** questions**,** with the intention to understand the nature and complexity of the processes taking place (Dooley, 2002; Yin, 2003; Creswell, 2005); and
- the **flexibility** that the case study research strategy presents to the researcher (Creswell, 2005).

The choice of a case study in this research indicates the researcher’s interest in a specific phenomenon and wishes to understand it completely, not by controlling variables but rather by observing all of the variables and their interacting relationships as suggested by Dooley (2002). The case study allows the use of any data collection methods, triangulation (Shanks & Parr, 2003; Creswell, 2005; Goldkuhl, 2012; Yin, 2003; Myers, 2011). This study uses a multiple of research methods within the data-generation process namely, participatory observation, physical inspection and interview. These techniques are to be used in conjunction with a particular information security risk management technique namely, OCTAVE-small.

The risk assessment and analysis method, OCTAVE-small, used in studying the information systems has a direct influence on the choice of the case study strategy. OCTAVE-small is a qualitative technique that requires data collection methods that allow the researchers to study the information systems through interactions with system users and the systems (Alberts and Dorofee, 2001). Such methods include observations, inspections, interviews and possibly workshops and brainstorming. This illustrates that this research methodology is suitable because the data collection techniques this study uses are similar to those used by the OCTAVE-small risk method. The OCTAVE-small method is discussed in detail in Chapter 6.

The main criticism of a case study research is its inability to generalise findings (Shanks & Parr, 2003; Stockdale & Standing 2006). Secondly, the case study is criticised for being difficult to design and evaluate according to the criteria of the natural science model of research which emphasises on controlled observations, controlled deductions, replicability and generalisability (Yin, 2003; Cresswell, 2005; Myers, 2011). These concerns have been discussed above under credibility, transferability, dependability and conformability in sub-sections 2.2.3.1 to 2.2.3.4.

A key feature of the design of the case study research is the number of cases included in a research study (Goldkuhl, 2008; Merriam, 2009; Myers, 2011). A case study research that intends to learn about a unique phenomenon utilises an intrinsic single case in which the researcher defines the uniqueness of this phenomenon which distinguishes it from all others (Crowe *et al*. 2011). Multiple cases are preferable when the purpose of the research is to describe phenomena, develop and test theories (Merriam, 2009; Myers, 2011).

This research study utilises the collective or multi-case study framework that would enable the researcher to study two secondary schools. The two schools will be drawn from the Thohoyandou Cluster in Vhembe District. This is done in an attempt to generate a still and broader appreciation of a particular issue (Crowe *et al*. 2011), in this case information security risk management in CISs in secondary schools.

2.2.8. Research design

Research design is the overall strategy that the researcher utilises to integrate different components of the study in a coherent and logical way, thereby ensuring that one will effectively address the research problem; it constitutes the blueprint for the collection, measurement, and analysis of data (De Vaus, 2001; Trochim, 2006). This research study utilises a qualitative case study design described in the preceding subsections of this chapter. The design being used in this study takes into account how data were to be collected, instruments to be employed, how the instruments were to be used and the intended means for analysing data collected. Subsequent subsections elucidate on the components of research design used in this study.

2.2.9. Qualitative data generation methods

Data generation is a step that follows research design as shown in Figure 2.1. The underlying principle in generating data in a case study research is that of triangulation, the use and combination of different methods to study the same phenomenon (Voss *et al*. 2002; Cresswell, 2005; Myers, 2011). This study uses a number of data generating methods namely participation observation, inspection and interview, which are the main methods of collecting qualitative data in a case study (Dooley, 2002; Cresswell, 2005; Crowe *et al*. 2011). The selected data collection methods facilitate direct interaction of the researcher and individuals in the research sample on a one to one basis or in a group setting (Hancock, 2002; Stockdale & Standing 2006).

Observation is a data collection technique in which the researcher collects data by watching the behaviours, events or noting physical characteristics in their natural setting (Creswell, 2005; Ritchie & Lewis, 2005, Evaluation Briefs, 2008). Participatory observation is the primary data generating method in this study. The use of participatory observation method gives the researcher an opportunity to collect data on a wide range of behaviours, to capture a great variety of interactions, and to openly explore the research topic (Hancock, 2002; Mark, Woodsong, Guest & Namey, 2005; Stockdale & Standing 2006).

In addition to participatory observation, this study utilises an interview designed to elicit a vivid picture of the participant's perspective on the research topic (Mark *et al*. 2005). **Interviews** are the means by which the researcher would best access case study participants' views and interpretations of actions and events (Darke, Shanks & Broadbent, 1998; Merriam, 2009). Interviews also enable the researcher to collect data on perspectives of research participants which are different from those collected using participatory observation method. The interview enables research participants to talk about their personal feelings, opinions and experiences on a topical issue (Mark *et al*. 2005; Maxwell, 2008). The data from interview would aid the researcher in gaining insight into how users interpret risks associated with their information systems.

Data collection methods used in a qualitative case study are time consuming and consequently data are collected from a smaller number of samples than when quantitative methods are used (Cresswell, 2005; Mouton, 2009). This study will use a purposive sample of two secondary schools which make use of CISs. Only the users of the CISs and of those computers they use form the population from which the research sample will be drawn.

Another major challenge of a qualitative case study relates to the researcher's ability to deal with large volumes of data (Cresswell, 2005; Merriam, 2009, Myers, 2011). This study utilises data management and analysis techniques suggested by Cresswell (2005), Oates (2006) and Merriam (2009) that include data preparation, data reduction, data analysis and interpretation or conclusion drawing.

Data **preparation** is the structuring of data into a format ready for analysis (Nienaber, 2008). Data from observations will be entered into computer files in tabular form while that from the interviews will be transcribed and then entered into computer files for easy readability and manipulation. After data preparation, the next step involves data analysis.

Data **analysis** is the process of making sense out of the data by consolidating, reducing and interpreting what people have said and what the researcher has seen and read (Merriam, 2009). Thorough analysis of data brings forth a clear understanding of various elements of these data. During this process, data are inspected to determine relationship among concepts, constructs or variables (Nienaber, 2008). Therefore, the major objective of data analysis is to identify or isolate any clear trends, patterns or even themes in the data (Nienaber, 2008; Merriam, 2009).

Qualitative data analysis consists of three concurrent flows of activities namely data reduction, data display and interpretation or conclusion drawing (Miles & Huberman, 1994). These three activities are interwoven before, during and after data collection and preparation (Gerber, 2006). Figure 2.2 shows that qualitative data analysis is continuous and interactive.

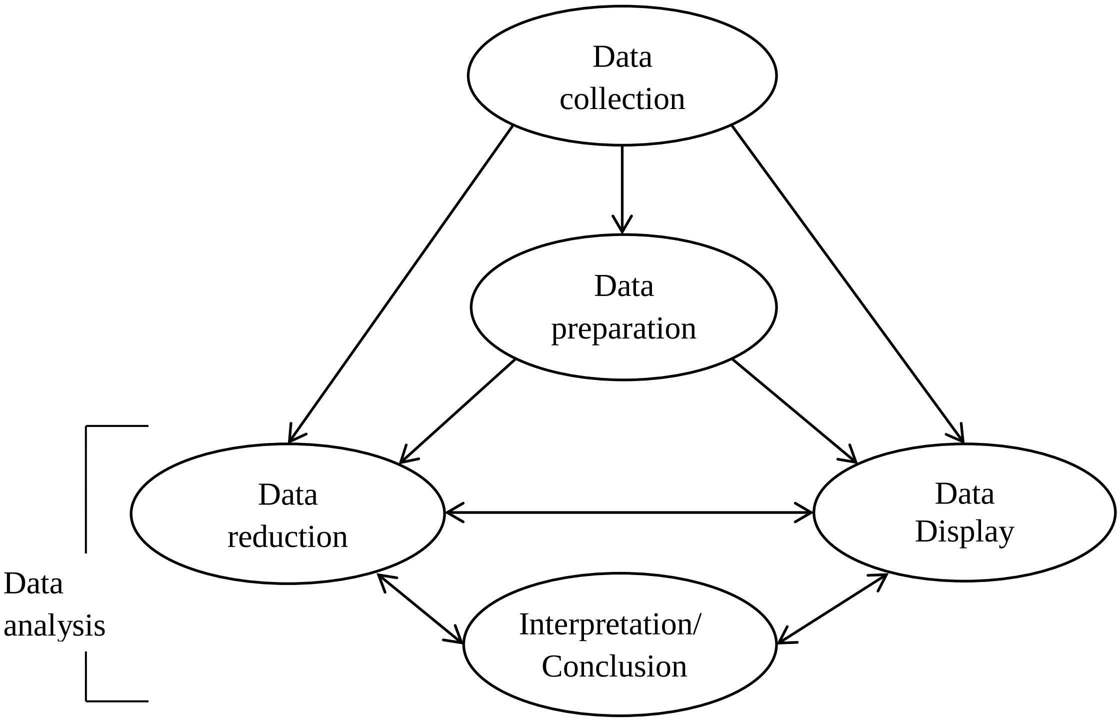


Figure 2.2: Interactive model of qualitative data analysis

Source: Miles and Huberman (1994)

Data **reduction** is the process of selecting, focusing, simplifying, abstracting and transforming qualitative data (Gerber, 2006). In this study data reduction will involve identification of broad themes within the research problem where relevant data would be further categorised and ordered by identifying broad categories and units as suggested by Marshall and Rossman (2006) and Nienaber (2008). This categorisation would be based on deductive approach, (data treatment guided by existing theories) or based on inductive approach where categories emerge purely from data explored (Nienaber, 2008; Mouton, 2009). Data categorisation leads to establishing interconnections among the categories that would be used for analysis.

Data display process involves assembling and organising information into accessible and compact form intended to draw conclusions (Gerber, 2006). To draw conclusions and verify the research findings, the researcher interprets the data in a more meaningful way. Data interpretation involves synthesising of research data based on identified trends, into larger coherent structures that could be used to formulate theories or hypothesis that reflect on observed patterns or trends in data (Nienaber, 2008). The researcher decides what the data mean (Gerber, 2006). Data analysis is based on a given method.

2.2.10. Data analysis method

The process of research presented in Figure 2.1 shows that this research study uses a qualitative data analysis method. This arises from the fact that this study will generate mainly qualitative data. The expected data forms would be mainly non-numerical, such as words, images, documents, tapes and researcher's notes on diaries and possibly memos (Cresswell, 2005; Nienaber, 2008; Merriam, 2009). This study uses data from participatory observation, inspections, interviews and possibly output documents from the CISs being studied.

2.2. SCOPE OF THE STUDY

This study addresses information security risk management in secondary schools' CISs. The purpose of the research study was to provide a set of guidelines to assist secondary schools to effectively manage information security risks in their computerised information systems. The study also established how secondary schools protected their CISs and then advocated for simple risk management solutions that non-technical personnel would easily apply to manage identified risks within their CISs. A case study research strategy was used and a risk management exercise was performed in two secondary schools' CISs using the OCTAVE-small technique. The study also concentrated on those information systems used for administrative purposes, their surroundings and the users of the systems.

2.3. CONCLUSION

A research study is normally conducted in the manner guided by the research methodology and philosophy subscribed to, the research strategy employed, data generating methods and research instruments utilised in the pursuit of the research objectives and the quest for the solution to the problem. The research methodology used in this dissertation has been implemented according to the research process suggested by Oates (2006). Table 2.2 is a summary of important components of the research methodology used.

Table 2.2: Dissertation research methodology

Research methodology	**This dissertation**
Research paradigm	Interpretive
Research strategy	Case study
Data generation methods	Participatory observation, inspections, interview, documents
Data analysis	Qualitative

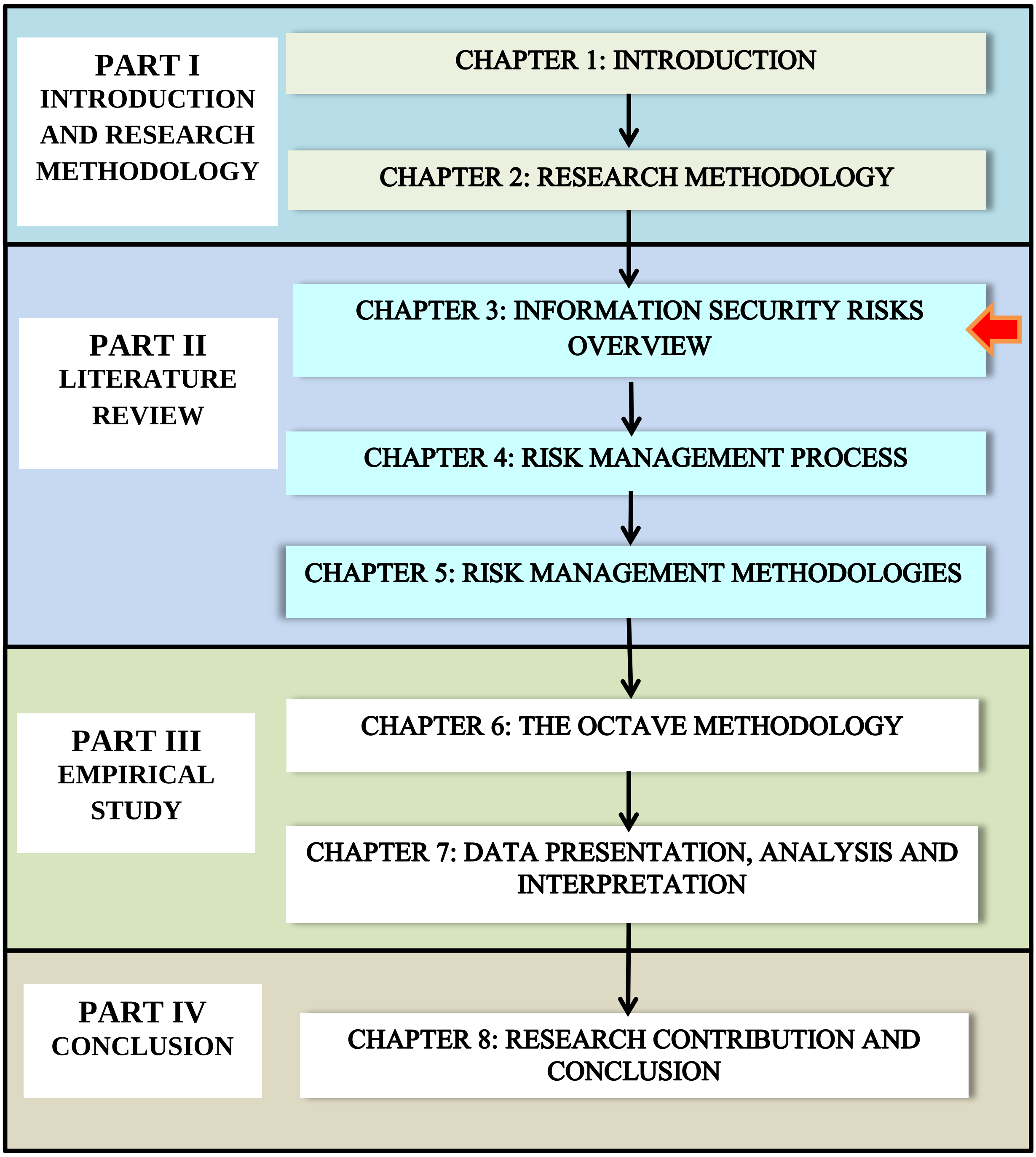
This chapter expands on the research methodology ideas outlined in the introductory chapter. A detailed account of research methodology to be implemented in this study has been given. It also links the research objectives to the research methodology and the risk assessment and analysis method, namely OCTAVE-small. Up to this point, this chapter has served the purpose of putting this research study into context. The next major section of this dissertation is Part II, Literature Review consisting of Chapters 3, 4 and 5.

PART II

LITERATURE REVIEW

CHAPTER 3

3. INFORMATION SECURITY RISKS OVERVIEW


PART I
INTRODUCTION AND RESEARCH METHODOLOGY
CHAPTER 1: INTRODUCTION
CHAPTER 2: RESEARCH METHODOLOGY
PART II
LITERATURE REVIEW
CHAPTER 3: INFORMATION SECURITY RISKS OVERVIEW
CHAPTER 4: RISK MANAGEMENT PROCESS
CHAPTER 5: RISK MANAGEMENT METHODOLOGIES
PART III
EMPIRICAL STUDY
CHAPTER 6: THE OCTAVE METHODOLOGY
CHAPTER 7: DATA PRESENTATION, ANALYSIS AND INTERPRETATION
PART IV
CONCLUSION
CHAPTER 8: RESEARCH CONTRIBUTION AND CONCLUSION

3.1. INTRODUCTION

All assets in an organisation are exposed to a certain level of risk due to various threats. Information systems assets seem to be the most affected. Threats to information systems assets may be due to natural events, accidents or intentional acts and tend to cause harm to these assets (Elky, 2009). Under these circumstances, managing information security risk becomes a big challenge for any organisation which deals with permanent, temporary storage or transfer of information (Tiwari, 2010). Regardless of the nature and source of threats, it remains the responsibility of the owners of assets to limit or manage risks from these threats to the extent possible. The best way of counteracting risks is by conducting a proper risk management exercise for the CISs.

The first step in attaining the objectives of this study was to gather data that was used to establish the types of information security risks to which secondary schools CISs were exposed to, and the security controls in place to counter each identified risk. In order to achieve these objectives, a detailed literature review was done on information security risks, threats and vulnerabilities.

Common threats and threat sources associated with CISs are presented. Information security breaches arising from some of the threats are also discussed from a global perspective and then contextualised to secondary schools situations. Possible security controls to these security threats are discussed in subsequent chapters. The chapter addresses research sub-objectives 1 and 2 formulated in Chapter 1.

The outline of this chapter is as follows: the introduction highlights important concepts of information security risks; a general overview of risk factors; threats, exposure and vulnerability. Information security breaches are also identified as the discussion unfolds. The conclusion summarises the main ideas of this chapter and then links with Chapter 4.

3.2. WHAT IS INFORMATION SECURITY?

Information security is

- the practice of ensuring that information is only read, heard, changed, broadcast and otherwise used by people who have the right to do so (Kite, 2009);

- the preservation of confidentiality, integrity and availability of information (Theoharidou *et al*. 2005);
- the methodology used to protect information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction. It pertains to the confidentiality, integrity, and availability of data in various forms (print, electronic, or other forms) and can be applied by any type of organisation (corporations, financial institutions, hospitals, military, and governments) (South African Centre for Information Security, 2010).

Confidentiality is the protection of information against theft and eavesdropping (Chen, 2009). **Integrity** is the protection of information against unauthorised modification and masquerade (Elky, 2006; Chen, 2009). **Availability** refers to dependable access of users to authorised information, particularly in light of attacks such as denial of service against information systems (Elky, 2006; Chen, 2009).

In this study, information security refers to the protection of all elements of an information system namely hardware, software, information, people and processes. The importance of information security increases as the use of and reliance on information by an organisation grows (Kite, 2009). Information security requires a range of skills and knowledge that are rarely found in small-scale organisations like high schools.

Information security and risk management are related to a number of important concepts that need to be explored. Section 3.4 is a detailed exploration of the important concepts.

3.3. INFORMATION SECURITY RISK, THREATS AND VULNERABILITIES

Literature reveals that consensus exists on what a risk is and clearly distinguishes it from a threat. A **risk** is the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the asset (Ciechanowicz, 1997). In this regard, a risk is the potential for an unwanted event to occur and is a function of the likelihood of that unwanted event occurring and its consequences (Siu, 2007). Tiwari (2010) substantiate this by arguing that an information security risk is any possible threat that exploits vulnerabilities in the asset of an organisation to cause disruption to the organisational routines and processes in one way or the other. Generally, a risk is any event, occurrence or actions that may prevent an organisation from realising its ambitions, plans and goals (Alhawari, Karadsheh, Talet & Mansour, 2012). A risk occurs when there is a likelihood of a given threat-source exercising a particular potential vulnerability in the asset, and results into an impact of adverse effect on the organisation (Elky, 2006). From these definitions, it could be argued that a risk is associated with a threat exploiting a potential weakness in the protection of an asset and has negative effects on the organisation concerned.

A risk arises from three conditions called risk factors (contextual problems), namely the existence of a **threat** (hazard), **exposure** of an asset to that threat and the **vulnerability** in the asset (Pare, Scott, Jaana & Giroud, 2008; Tiwari, 2010; Alhawari *et al*. 2012). A threat can be a natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property (United States of America Department of Home Security DHS, 2010). The existence of a threat implies that there exists the capability and intention of an adversary to undertake actions that could be detrimental to an organisation's interests (Elky, 2006). A threat transforms to a hazard when presented with an opportunity to utilise an asset's existing vulnerability. In this case a hazard is a single event or series of events characterised by the magnitude and likelihood of occurrence (Metras, 2008). Hazardous conditions or events can be triggered by nature, intentionally or accidentally by humans, which could cause disruptions, harm or loss of service provided by an information system. Figure 3.1 shows the Crichton (2009) risk triangle of hazard, exposure and vulnerability commonly used to show the relationship that leads to risk.

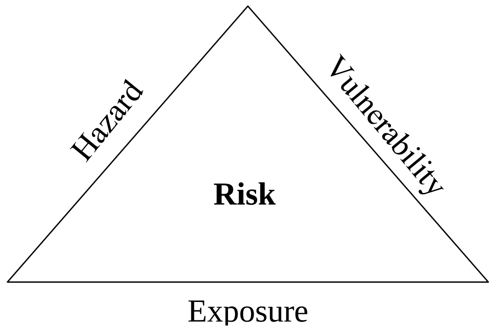


Figure 3.1: The risk triangle
Source: Crichton (2009)

An information security exposure is a system configuration issue, mistake in software or a problem according to some reasonable security policy that allows access to information or capabilities that can be used by an attacker as a stepping stone into the system or network (Common Vulnerabilities and Exposures CVE, 2012). Exposure refers to the state of leaving an asset without protection against something harmful. In this case an asset is in the condition of being subject to some detrimental effect or harmful condition (Aven, 2012). Crichton's risk triangle suggests that the broader the base of the triangle (exposure) the greater the risk to which an asset is exposed. A threat can only attack an asset if a vulnerability, a flaw or weakness exists in that asset and could be exploited by an adversary to cause damage to an organisation's interests (Tiwari, 2010). Vulnerability is a combination of the attractiveness of a facility as a target and the level of deterrence and (or) defence provided by the existing security controls (Renfroe & Smith, 2011). Therefore, vulnerability is the degree to which the exposed elements of an information system will suffer a loss, from the impact of a hazard. A threat-source does not present a risk when there is no vulnerability that can be exercised (Stoneburner *et al*. 2002).

This discussion indicates that information systems assets are always at risk and it is imperative for information systems users to be aware of the types of risks so that appropriate decisions are made to safeguard the assets for the smooth running of an organisation.

The Crichton risk triangle plays a vital role in this study as it illustrates the link between threats to information systems assets, their exposure to these threats and vulnerabilities that could be exploited by threats. To aid the Crichton triangle is the United States Department of Commerce Office of Security OYS (2011) conception of asset, threat and vulnerability links that lead to risk, shown in Figure 3.2. This is based on the formula:

Risk = Impact x (Threat x Vulnerability).

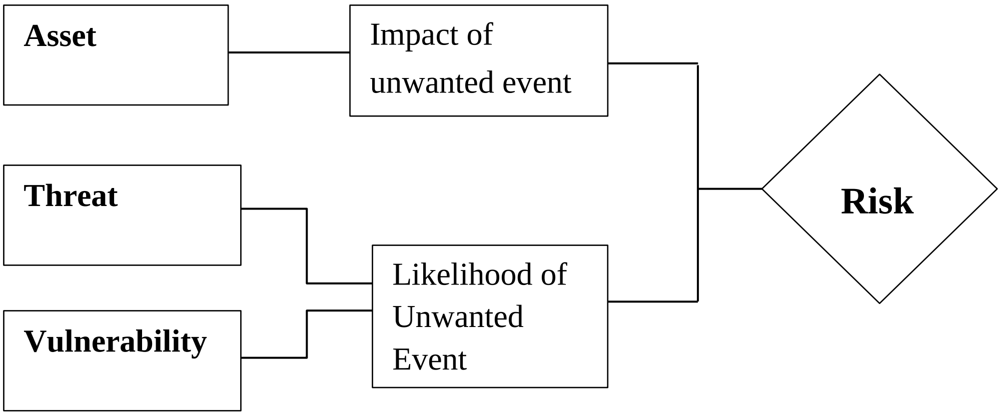


Figure 3.2: Asset, threat and vulnerability diagram
Source: OSY (2011)

Vulnerabilities in information systems' assets are apportioned to flaws or weakness in system security procedures, design, implementation or internal security controls that are likely to be exploited and result in security breaches or a violation of the system's security policy (Elky, 2006; Goel & Chen, 2008; Tiwari, 2010). In the long run, the flaws in the information asset are likely to be accidentally triggered or intentionally exploited by threats.

The following section is a brief outline of common information systems assets likely to be found in various organisations.

3.4. COMMON INFORMATION SYSTEMS ASSETS

An information system asset is anything of value that an organisation needs in order to accomplish its mission (Ciechanowicz, 1997). Information systems comprise of both tangible and intangible assets (Goel & Chen, 2008). Tangible assets include software, hardware and data while intangible assets include reputation, operations, trust and morale

(Tohidi, 2010), and information technology services (Microsoft TechNet, 2006). There are critical and non-critical information system assets depending on how important are the operations that each asset is supporting. These vary from organisation to organisation (Goel & Chen, 2008). Security breaches of more critical assets have greater effects, damage or disruptions to the operations of the organisation, than less or non-critical assets (Goel & Chen, 2008). Literature surveyed indicates that some of the information systems assets found in small-scale organisations match those found in large-scale organisations.

Microsoft TechNet (2006) provides a comprehensive list of common information systems assets and their ratings. Table 3.1 is a customised list of common information systems assets in various organisations. The asset values used are based on how critical an asset is in the attainment of organisational objectives.

Table 3.1: Common information systems assets

Asset class	Name	Description	Asset value
Tangible	Servers	Hardware	Critical
	Desktop computers	Hardware	Non-critical
	Mobile computers	Hardware	Critical
	Cell phones	Hardware	Non-critical
	End-user application software	Software	Non-critical
	Routers	Hardware	Critical
	Antiviruses	Software	Critical
	Network switches	Hardware	Critical
	Operating systems	Software	Critical
	Firewalls	Software / hardware	Critical
	Removable media (tapes, CD-ROMs, DVDs, portable hard drives, PC card storage devices, USB storage devices)	Hardware	Non-critical
	Power supplies	Hardware	Critical
	Uninterruptible power supplies	Hardware	Non-critical

Asset class	Name	Description	Asset value
	Air conditioning systems	Hardware	Critical
	Air filtration systems	Hardware	Non-critical
	Other environmental control systems		Non-critical
	Human resources data	Information	Critical
	Financial data	Information	Critical
	Employee passwords	Information	Critical
	Employee personal contact data	Information	Non-critical
Intangible	Reputation		Critical
	Goodwill		Non-critical
	Employee moral		Non-critical
	Reputation		Critical
	Employee productivity		Critical
Services	E-mail/scheduling		Non-critical
	Instant messaging		Non-critical
	Enterprise management tools		Critical
	File sharing		Critical
	Storage		Critical

Source: Microsoft TechNet (2006) - Customised

This list forms the basis on which secondary schools' CISs assets will be identified. The next section discusses common information security threats and possible sources.

3.5. COMMON INFORMATION SECURITY THREATS AND SOURCES

Information security risks have been found to be a result of many different threats-sources such as natural disasters, security breaches, poorly designed software, third-party vendors, unstable computing environment and project fail-users (Elky, 2006; Alhawari *et al*. 2012). Authors in information security categorise these various information security threats as natural, human or environmental threats (Kite 2009). Elky (2006) provides a summary of common threats to information security in CISs regardless of the nature and size of an organisation. Table 3.2 is a summary of common security threats and sources

Table 3.2: Common threats to information security

Threat/threat sources	**Description**
Acts of nature	All types of natural occurrences (earthquakes, floods, fire) that may damage or affect an information system or application. Any of these potential threats could lead to a partial or a total system outage, thereby affecting availability
Accidental disclosure	The unauthorized or accidental release of classified, personal, or sensitive information that affects confidentiality
Intentional alteration of software or alteration of data	An intentional modification, insertion, deletion of operating system or application system programs, whether by an authorised user or not. This compromises the confidentiality, availability, or integrity of data, programs, system, or resources controlled by the system.
Bandwidth usage	The accidental or intentional use of communications bandwidth for other than intended purposes.
System configuration error (accidental)	An accidental configuration error during the initial installation or upgrade of hardware, software, communication equipment or operational environment.
Malicious software and infections	Use of malicious code, such as logic bombs, Trojan horses, trapdoors, and viruses infect crucial system files and data. This compromises confidentiality, integrity and availability.
Theft of data or computer hardware	Unauthorised copying of personal information or records by an individual. Physical removal of computing hardware from designated points without authorisation, or through burglary.
Telecommunication malfunction/ interruption	Any communications link, unit or component failure sufficient to cause interruptions in the data transfer via telecommunications between computer terminals, remote or distributed processors, and host computing facility.
Electrical interference/ disruption	An interference or fluctuation may occur as the result of a commercial power failure. This may cause denial of service to authorized users (failure) or a modification of data (fluctuation).

Source: Elky (2006)

Most of the threats shown on Table 3.2 pose information security breaches and may cause risks security in information systems (Cate, 2005; Potter & Beard, 2010). Small-scale organisations, particularly schools may find it difficult to identify or detect and decisively deal with threats/threats sources before they impact negatively on the information systems.

3.6. INFORMATION SECURITY BREACHES

An information security breach is a situation where an individual intentionally exceeds or misuses network, system, or data access in a manner that negatively affects the security of the organisation's data, systems, or operations (Kassner, 2009). Information security breaches in an organisation take many forms and occur in a wide variety of settings depending on the intention of the attacker and the possible existing vulnerabilities (Cate, 2005). The most prevalent information security breaches on large and small-scale organisations as identified by Cate (2005), Kite (2009), Schmidt (2011), and Potter and Waterfall (2012) are summarised below:

- system failure or data corruption (Kite, 2009);
- infection by viruses or other malicious software (Kite, 2009; Potter &Waterfall, 2012);
- theft or fraud involving computers, for example a person stealing an unsecured organisation laptop containing personal information (Cate, 2005; Kite, 2009);
- other incidents caused by staff employed by the organisation (Cate, 2005);
- attacks by an unauthorised outsider (including hacking attempts) on an organisation's computerised records containing personalised information; and
- an organisation disposing off records containing personal information into a trash dumpster without properly destroying the personal information by shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or indecipherable through any means (Schmidt, 2011; Potter & Waterfall, 2012).

A technical report on security breaches by Potter and Waterfall (2012) indicates that small-scale organisations also suffer from major security breaches. The report alludes to the use of social networks and externally hosted software services as having moved the Internet use beyond just websites and email but as a vehicle to change the computing environment. However, Potter and Waterfall (2012) also argue that the changing computing environment has created new vulnerabilities, which criminals are adapting their techniques by exploiting these vulnerabilities.

Small-scale organisations, such as secondary schools are likely to fall prey to some of these security breaches through commission, omission, oversight or ignorance on the part of the school management and users of CISs. Individuals, who access school information systems, authorised or not, have different motives likely to have serious consequences on these assets. Table 3.3 lists possible vulnerabilities.

Table 3.3: List of vulnerabilities in information systems assets

High level vulnerability class	**Brief description of the vulnerability**
Physical	Unlocked doors Unguarded access to computing facilities Insufficient fire suppression systems Flammable materials used in construction Flammable materials used in finishing Unlocked windows Walls susceptible to physical assault Interior walls do not completely seal the room at both the ceiling and floor Facility located in a flood zone
Hardware	Missing patches Out-dated firmware Misconfigured systems Systems not physically secured Management protocols allowed over public interfaces
Software	Out of date antivirus software Missing patches Poorly written applications
	Deliberately placed weaknesses • Vendor backdoors for management or system recovery • Spyware • Trojan horses
	Configuration errors • Manual provisioning leading to inconsistent configurations • Systems not hardened • Systems not audited

High level vulnerability class	**Brief description of the vulnerability**
	• Systems not monitored
Media	Electrical interference
Communications	Unencrypted network protocols Connections to multiple networks Unnecessary protocols allowed No filtering between network segments
Human	Poorly defined procedures Insufficient incident response preparedness Manual provisioning Insufficient disaster recovery plans Testing on production systems Violations not reported Poor change control Stolen credentials

Source Microsoft TechNet (2006) -Customised

During the proposed risk assessment and analysis exercise, this study will also attempt to ascertain whether these vulnerabilities exist in secondary schools' computerised information systems assets.

3.7. CONCLUSION

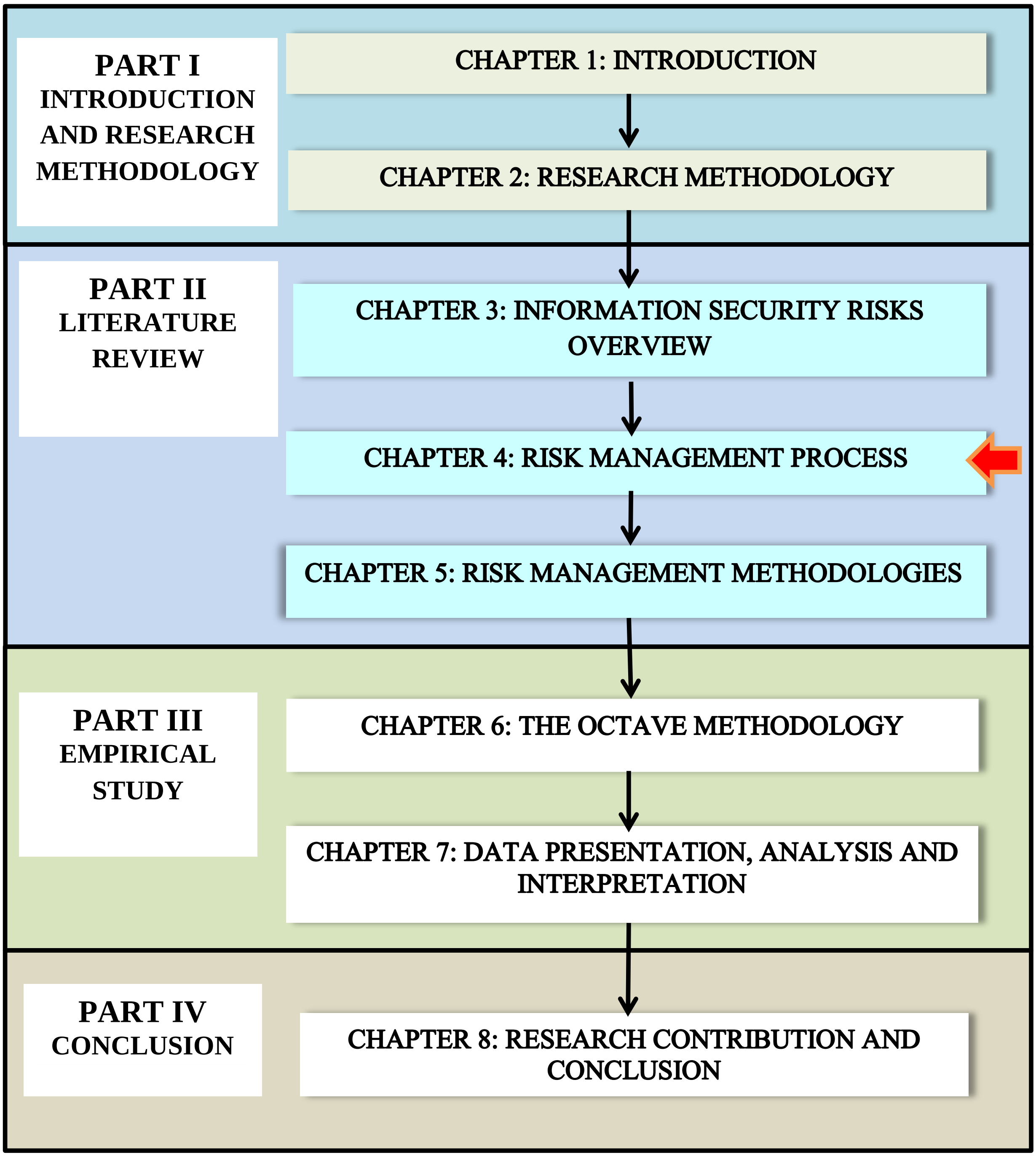
This chapter discussed information security risks and cited a number of security threats and breaches most likely to impact negatively on an information system regardless of the nature and size of the concerned organisation. The literature reviewed shows that a tripartite link of threat, exposure and vulnerability to information systems assets could lead to risks. The types of information security risks, threats, exposures and vulnerabilities that exist within the context of an organisation were delineated in an effort to determine the factors that drive such risks. Security breaches have been described as either intentional or unintentional. The discussion indicates that human beings are the major cause of security threats and breaches in organisations that use CISs.

In an attempt to achieve the objectives of this study, this chapter forms the basis for subsequent chapters to explore different types of threats, exposures and vulnerabilities.

Chapter 4 discusses the risk management process alluding to a standardised framework, the AS/NZS ISO 31000:2009 before exploring the OCTAVE-small risk method in Chapters 5 and 6. This is intended to examine the process of risk management using a framework which allows integration of any risk management methodology to practically perform risk management exercise.

CHAPTER 4

4. RISK MANAGEMENT PROCESS


PART I
INTRODUCTION AND RESEARCH METHODOLOGY
CHAPTER 1: INTRODUCTION
CHAPTER 2: RESEARCH METHODOLOGY
PART II
LITERATURE REVIEW
CHAPTER 3: INFORMATION SECURITY RISKS OVERVIEW
CHAPTER 4: RISK MANAGEMENT PROCESS
CHAPTER 5: RISK MANAGEMENT METHODOLOGIES
PART III
EMPIRICAL STUDY
CHAPTER 6: THE OCTAVE METHODOLOGY
CHAPTER 7: DATA PRESENTATION, ANALYSIS AND INTERPRETATION
PART IV
CONCLUSION
CHAPTER 8: RESEARCH CONTRIBUTION AND CONCLUSION

4.1. INTRODUCTION

Risk management is a basic management activity that helps an organisation to meet its objectives through the allocation of resources to undertake planning, make decisions and carry out productive activities (Shortreed, Hicks & Craig, 2003). With the aid of a risk management process, secondary schools can identify risks, perform risk assessment and analysis, and then put in place possible security controls to reduce or eradicate the risks in their CISs. Unlike other management activities, risk management focuses on a number of issues with uncertainties that managers have to deal with. These uncertainties include, as cited by Shortreed *et al*. (2003):

- uncertainties that an organisation faces on a daily basis;
- uncertainties in the probability of occurrence of events;
- uncertainties in the value to the organisation of consequences of events; and
- other uncertainties that fall outside the normally expected range of variation.

It becomes imperative for an organisation to conduct a risk management exercise so that the management has a clearer picture of the impending risks to which its assets are exposed. A risk management exercise is carried out within a risk management framework using appropriate risk management methodologies and tools (Shortreed *et al*. 2003; Elky, 2006). In view of this argument, this study used the AS/NZS ISO 31000:2009 risk management framework.

A risk management framework is an essential philosophy for approaching any security work (McGraw, 2005). A risk management framework is a description of an organisational specific set of functional activities and associated definitions that define the risk management system in an organisation and the relationship to the risk management organisational system (Shortreed, 2008). Therefore, a risk management framework defines the processes and the order and timing of processes that will be used to manage risks. There are many information security risk management frameworks available today applicable to different situations. The AS/NZS ISO 31000:2009 is one such information risk management framework that has been used in various circumstances with much success as reported in a number of studies.

The purpose of this chapter is to discuss a risk management framework including its processes as exemplified by the AS/NZS ISO 31000:2009 risk management framework and describe how the framework will be used with a selected information security risk assessment and analysis tool, namely the Operationally Critical Threats, Assets and Vulnerability Evaluation for small-scale organisations (OCTAVE-small).

The structure of this chapter is as follows: the introduction, risk management definitions, an insight into the AS/NZS ISO 31000:2009 framework, concentrating on the risk management process. Components of the framework which are important to this study are examined under different subtopics.

4.2. RISK MANAGEMENT

Different authors define risk management differently. Risk management is:

- a systematic and analytical process whereby an organisation identifies, reduces and controls its potential threats and losses (Stoneburner *et al*. 2002);
- a process of identifying, controlling and minimizing or eliminating security risks that may affect information systems for an acceptable cost (Theoharidou *et al*. 2005);
- a systematic application of management policies, procedures and practices to the tasks of communicating, consultation, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk (Shortreed , 2008);
- a systematic process of setting the best course of action under uncertainty by identifying, assessing, understanding, acting on and communicating risk issues (Tiwari, 2010; Tohidi, 2010).

In this study, risk management is defined as an on-going systematic process carried out by an organisation in order to identify, analyse, assess, evaluate, monitor and communicate risks in its information system assets with the aim of putting in place mechanisms to reduce the loss due to threat attacks when they occur.

The principal goal of information security risk management is to help an organisation better manage risks associated with its missions by ensuring the implementation of correct data security standards (Tohidi, 2010). A properly conducted risk management programme allows an organisation to determine the magnitude and effects of the potential loss, the likelihood of such a loss actually happening and security controls that could lower the probability or magnitude of loss (Tiwari, 2010). Regardless of the size of an organisation, the management should understand what risk is, its causes and how to mitigate it when there is a high chance of the occurrence of an attack. Schools should be prepared to use the risk management processes to identify and reduce risks associated with their CISs assets.

To undertake this feat, an appropriate risk management framework should be put in place prior to selection of the risk management tools to be used. The following section scrutinises a given risk management framework, AS/NZS ISO 31000:2009.

4.3. RISK MANAGEMENT FRAMEWORK

There are several models of information security risk management processes in use today. The majority of such models are suitable for large and commercial organisations that have strong financial bases. One of the most popular risk management models is the AS/NZS 4360:2004, now AS/NZS ISO 31000:2009. The AS/NZS ISO 31000:2009 risk management process consists of three major elements; a *risk management workflow*, *monitor and review*, and *communication and consult*. The latter two continuously interact with the steps of the risk management workflow. The *risk management workflow* comprises of a sequence of steps that an organisation has to undertake when exercising a risk management programme. The first step in the workflow is establishing context, followed by risk assessment, subdivided into risk identification and risk analysis, and risk evaluation.

The model in figure 4.1 depicts the risk management as an iterative and cyclic process. Rainer *et al*. (1991) cite two reasons why the risk management process is cyclical: the presence of new external threats for information systems assets generated by the changing computing environment, and new internal threats which are exposed by the security surveillance and audit process on information technology assets. These authors encourage the management to periodically conduct risk management exercises to re-evaluate the organisation's exposure to threats that may cause loss.

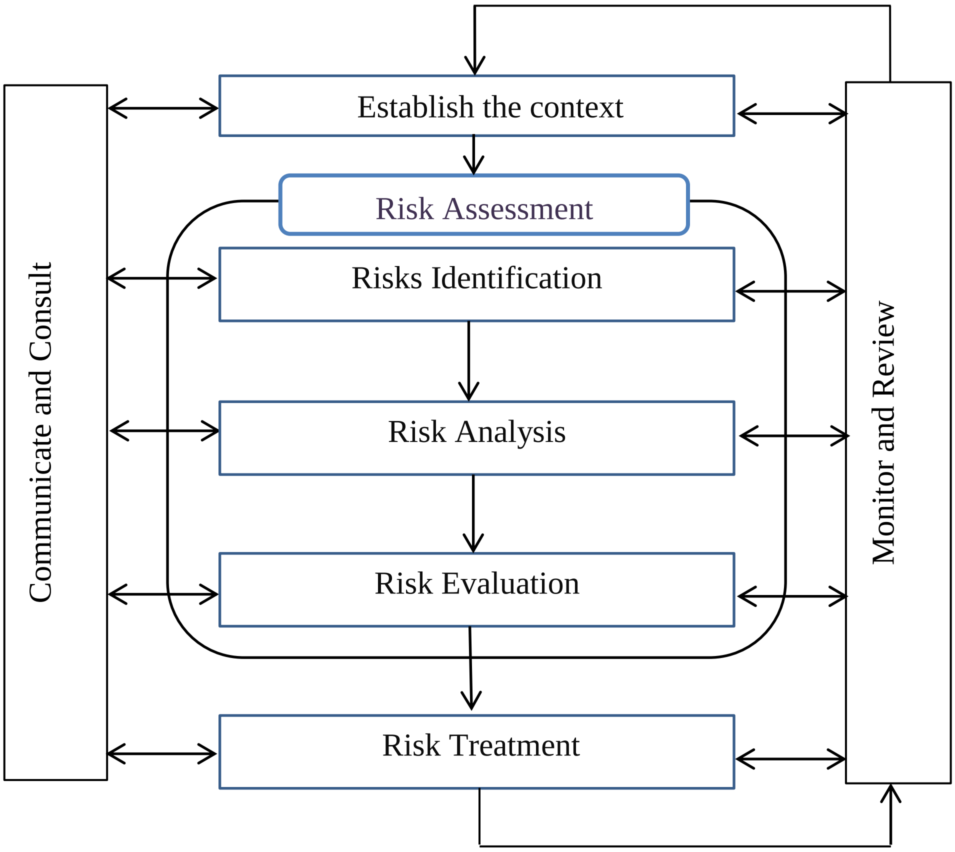


Figure 4.1: AS/NZS ISO 31000:2009: The model of risk management process

The AS/NZS ISO 31000:2009 major components are briefly discussed in subsections below.

4.3.1. Establishing the risk management context

The first step in risk management is to establish the context for information security risk management within an identified organisation, in this case the secondary schools. This process helps the risk management team to understand the structure, capabilities, goals, strategic objectives and operational processes of the concerned organisation (Elky, 2006; Tiwari, 2010). Establishing context means defining the bounds of what one wants to analyse for risks, whether a strategic or operational plan, industrial or administrative process, program, project of other management initiative (Edwards, 2010). When management establishes the context, it seeks to articulate an organisation's objectives, defines the external and internal parameters to be taken into account when managing risks, and sets the scope and risk criteria for the remaining processes (Brass, 2011). The importance of establishing the context for any risk assessment is based on the fact that the risk assessor is most likely to develop a thorough understanding of the environment in which an organisation exists and operates (Wawrzyniak, 2006; Brass, 2011). This also provides the framework for managing the risk management process itself. The output of establishing of context is the scope statement that sets the general parameters for undertaking the risk management process.

4.3.2. What is risk assessment?

Risk assessment in information security is a means of providing decision makers with information needed to understand factors that can negatively influence operations and outcomes and make informed judgments concerning the extent of actions needed to reduce risk (GAO/AIMD-00-33, 1999). Similarly, Hoo (2000) regards risk assessment as the process of identifying, characterising, and understanding risks; that is, studying, analysing, and describing the set of outcomes and likelihoods for a given endeavour. In the AS/NZS ISO 31000:2009 risk assessment is depicted as a three-step process that comprises of identifying, analysing and evaluating risks. This means that risk assessment is the overall process of identifying the sources of potential harm (hazard) and assessing both the seriousness (consequences) and the likelihood of any adverse outcome that may arise (Meek, 2005).

During risk assessment the risk management team identifies all sources of potential harm to their information systems assets. Once all risks have been identified the team then analyse each risk by assessing the chances of the occurrence of each identified harm and the consequences if harm does occur (Meek, 2005). A risk assessment exercise also involves evaluating existing physical, environmental security and security controls by assessing their adequacy relative to the potential threats of the organisation (Wold & Shriver, 1997; O'Donnell & Best, 2005). This implies that an assessment goes further than an analysis by including an evaluation whose main objective is to quantify or qualify the results of the analysis examination with regard to the exposure of the assets to the hazard (Elky, 2006; Kirupakar, 2007; Siu, 2007). Secondary schools can utilise risk assessment as a means of auditing the potential for unwanted situations to occur within their CISs. This may enable school management to make concrete decisions on steps which should be taken in order to minimise the possibility of the situation arising, thereby preserving the reputation of the school.

An effective risk assessment leads to the development of effective and informed risk management strategies which in turn reduce the likelihood of serious incidents and/or losses and could thereby significantly reduce costs (Wold & Shriver, 1997; O'Donnell & Best, 2005; Kirupakar, 2007). Therefore, risk assessment seeks to establish the level of risks so that appropriate protection measures are taken to reduce the risk to a level acceptable to the management of the organisation or to eliminate all risk if possible (Broderick, 2001; Elky, 2006; Tiwari, 2010). The first step in risk assessment is risk identification, discussed in subsection 4.3.2.1 below.

4.3.2.1. Risk identification

Risk identification is a deliberate and systematic effort to identify and document key risks in an organisation (National Treasury Republic of South Africa NTRSA, 2007). The main objectives of risk identification are to identify, categorise and document risks that could affect the information system of an organisation (Federal Highway Administration FHWA, 2007; Carothers, 2009). This activity enables management to understand what is at risk within the context of an organisation’s explicit and implicit objectives at the same time generating a comprehensive inventory of risks based on the threats and events that might prevent, degrade, delay or enhance the achievement of the objectives (NTRSA, 2007). By performing a risk identification exercise beforehand, secondary schools would benefit by preventing potential disruptions in their operations due to threat attacks.

The risk identification process results into specific deliverables, namely information security risk and critical registers, which are used as the foundation for the risk analysis (Elyse, 2007; Carothers, 2009). The register is a list of all possible risks, their location, time frame, root causes, and scenarios (GAO/AIMD-00-33, 1999; FHWA, 2007; Panda, 2009). The implication is that an organisation can hardly have an accurate active risk management strategy unless there is a risk identification process.

A number of techniques are used in a risk identification process. Carothers (2009) cites ten risk identification techniques frequently used in information systems security risk management in different types of organisations. After a critical analysis and matching of each technique to what this research intends to achieve only seven techniques seem to be viable. These are checklists, physical inspection, and brainstorming, interviewing system users, observing the system flaws during operations, flowcharts, and procedures and policies (Carothers, 2009).

Checklists are the most commonly used method of identifying information security risks (Taylor & Azadegan, 2007). These tools allow systematically identification of as many exposures, perils, and hazards as possible (Carothers, 2009). Checklists are standardised, therefore their use reduces human errors when identifying risks and this makes them easy to use by non-risk management personnel with minimal training (Taylor & Azadegan, 2007). Well-developed checklists can serve as reminder lists and help researchers to ensure consistency and completeness in the risk identification exercises (Taylor & Azadegan, 2007; Toolsjournal, 2010). Therefore, the use of security checklists could also reduce the chances of omitting key security features. Due to lack of risk management expertise in secondary schools, checklists seem to be one of the most appropriate techniques for identifying information security risks in CISs. However, the use of checklists as the only method of risk identification is associated with a number of disadvantages. Taylor and Azadegan (2007) argue that using checklists leads to over-reliance on an enumerated list that may lead to the idea that once the checklist is complete, risk identification is also complete. Secondly, if these tools were poorly developed or incomplete, their effective use in identifying security risks would be questionable (Steele & Wargo, 2007). Another weakness for information security checklists is that they hardly cover all areas or operations because they do not prioritise information security exposures that they identify especially new security exposures or flaws (Carothers, 2010). Despite these weaknesses, checklists remain valuable tools in this research and will be used in conjunction with other risk identification methods in the initial risk identification stage.

Physical inspection is another useful method for identifying risks in an information system where risk assessment is being conducted for the first time (Taylor & Azadegan, 2007). The use of physical inspection techniques allows the risk assessors to have face-to-face conversation with the users of the information systems at their work places (Carothers, 2009). This affords the risk the researcher an opportunity to have a very clear and precise picture of the risk environment of the organisation in which CISs are being used. Physical inspections present the risk assessor with a chance to find new hazards in an information system (Toolsjournal, 2010). The commonly used physical inspection technique of risk identification is a physical walk-about inspection of the operations in a work area or by observing the work, methods and tasks being performed within a workplace (Department of Environmental Affairs and Tourism DEAT, 2006). Physical inspections can help the researcher to observe the activities or operations performed by CISs users that are likely to pose as threats to these information systems. Secondly, physical inspections place the researcher in a better position to observe the computing environments that pose as threats. The researcher also gets an opportunity to discuss with the CISs users about their operating environment and information security problems they encounter that always impact negatively on their work. The drawback of physical risk inspection is that it is expensive in terms of time and money (Elky, 2006; Toolsjournal, 2010), and the results may become doubtful due to changes in the location or process being investigated (DEAT, 2006). However, in this research, the locations and processes being studied will remain unchanged for a longer period of time. This will make the use of physical inspection in conjunction with the checklist technique very useful.

A substantial discussion of the participatory observation and interview methods has been made in Chapter 2 as a result the next subsection focuses on risk analysis.

4.3.2.2. Risk analysis

Risk analysis is a crucial step in risk assessment which follows immediately after risk identification. The process of risk analysis involves further identifying security risks, determining their magnitude and identifying the corresponding areas that need security controls (Ciechanowicz, 1997). Risk analysis makes it possible to identify the most probable threats to an organisation and analyse the related vulnerabilities of the organisation to those threats (Wold & Shriver, 1997). Therefore, information security risk analysis is a multi-step process of determining exposure to security threats that an organisation faces (Goel & Chen, 2008). Risk analysis is based on threat and vulnerability analysis (Siu, 2007; Tiwari, 2007). Threat analysis is an examination of possible threats to each asset while the vulnerability analysis looks at the weaknesses in security that might enable a successful attack against the assets (Hoo, 2000; Goel & Chen, 2008). The output of risk analysis is the likelihood of a risk and the consequence in case of risk occurrence (Siu, 2007).

Although risk analysis is a complex process, there is an underlying mechanism that supports common sense paradigm (Ciechanowicz, 1997). This paradigm postulates that if a set of assets is of high value to an organisation and if the likelihood of a threat occurring is high and if there is a vulnerability that can be easily exploited by the threat then the level of risk is high (Ciechanowicz, 1997; Putvinski, 2012). Similarly, if a set of assets is of low value to an organisation and if the likelihood of a threat occurring is low and if there are no vulnerabilities that can be exploited by the threat then the level of risk is low (Ciechanowicz, 1997; Putvinski, 2012).

The common sense paradigm can be used in determining dependencies between assets, threats, and vulnerabilities either qualitatively through less expert opinions or quantitatively using empirical data subjected to rigorous mathematical computations (Goel & Chen, 2008). This paradigm is a simpler technique that can be used to determine whether a critical information systems asset being examined is under security threat or not. A risk analysis process culminates to a risk evaluation exercise which provides information used by school management to make decisions on what steps to take in view of identified risks. Risk evaluation is the subject of subsection 4.3.2.3 which follows.

4.3.2.3. Risk evaluation

Risk analysis provides an outcome which is a basis for decision making on which risks need treatments and in which priority they should be treated. Therefore, risk evaluation is the process of comparing the results of risk analysis against risk criteria to determine whether the level of risk is acceptable or tolerable (Shortreed, 2008). The main purpose of evaluating risks is to determine whether the risks which have been identified are acceptable or unacceptable. Any risk determined to be acceptable should be monitored and periodically reviewed to ensure it remains acceptable (Australian Capital Territory Insurance Authority ACTIA, 2004). On the other hand, risks regarded as unacceptable should be treated immediately using risk treatment strategies or putting in place appropriate security controls reducing the risk to acceptable levels (ACTIA, 2004).

After the completion of a risk assessment process information system users and the management are expected to understand:

- what is at risk;
- the assets and value at risk - as associated with the identity of information assets and with the confidentiality, availability, and integrity of information assets;
- the kinds of threats that could occur and consequences associated with them;
- risk mitigation analysis. What can be done to reduce risk to an acceptable level;
- risk mitigation costs and associated cost; and
- whether suggested risk mitigation activities are cost-effective (ACTIA, 2004; Shortreed, 2008).

An effective risk assessment and analysis method assists an organisation to determine the appropriate security controls to meet its information security needs. However, in real world risk evaluation scenarios make it difficult for risk analysts to work out the complex relationships between security controls (Lo & Chen, 2012). Risk analysts from diverse backgrounds produce subjective assessments and analyses based on their specialised standing, duties and job positions (Lo & Chen, 2012). Therefore, schools have to do their own risk assessments and analysis depending on the expertise and information systems assets at their disposal. The process of risk evaluation leads to decisions on risk treatment, a decisive step in the risk management programme. The immediate subsection 4.3.3 is dedicated to risk treatment.

4.3.3. Risk Treatment

Risk treatment is a process that consists of selecting and applying the most appropriate risk controls in order to be in a position to modify the risk, with the aim of avoiding the damages intrinsic to the risk factor or of making use of the advantages it could provide the organisation (Hoo, 2006; Shortreed, 2008). Literature on risk management discusses four prominent risk treatment strategies that are commonly used; risk avoidance, acceptance, transference and treatment (ACTIA, 2004; Meek, 2005; Elky, 2006; Dorian, 2012). The main objective of risk management is the implementation of appropriate risk mitigation, risk transfer and risk recovery measures to reduce business exposure by balancing control investment against risk (Abdullah, 2006). The knowledge of these risk treatment strategies is important in assisting management in selecting the most appropriate strategy for an identified risk in their computerised information system. The following subsections briefly discuss each treatment strategy.

4.3.3.1. Risk avoidance

Risk avoidance is the practice of removing the vulnerable aspect of the system or even the system itself (Elky, 2006), because some risks may only return to acceptable levels if the activity is terminated (The State of Queensland TSQ, 2011). Risks to information systems exist from many known and unknown threat-sources and as a result attempting to avoid it becomes virtually impossible. It is extremely difficult for an organisation to avoid risks to its sensitive information while still providing access to authorised users, applications and systems (Navarro, 2001). This situation applies to secondary schools where risk avoidance may be difficult due to the fact that a number of users access the school network for a number of reasons. Therefore, the management should explore other risk treatment strategies.

4.3.3.2. Risk acceptance

Risk acceptance is the practice of simply allowing the system to operate with a known risk (Elky, 2006). This normally applies to:

- low risks that are most likely not to cause any disruptions in the near future; and
- those risks that have an extremely high cost to mitigate.

When an organisation decides to accept a risk, it does so with the knowledge that, should a particular vulnerability be exploited, the impact on this organisation is such that the organisation will continue despite this impact (Navarro, 2001). Risk acceptance by secondary schools should be based on informed decisions on the likely consequences of such an option.

4.3.3.3. Risk transference

Risk transference is the process of allowing one party to accept the risk on behalf of another (Elky, 2006). When this strategy is used an organisation transfers or shares the risk with a third party, normally a trusted security company (Navarro, 2001). The trusted security partner takes on some of the information security risks. This enables the affected organisation to concentrate on its core activities with reduced risks. This has cost obligations for both organisations. The protected organisation pays for the security services offered while the security provider also pays for any loss incurred by the protected organisation. Some organisations insure their computing assets and the insurance company replaces all damaged equipment. This setup is suitable for profit making organisations as the insurance organisations might make demands that schools might find too exorbitant to meet. It is difficult for schools to transfer risks due to these costs. This might force schools to avoid, accept or attempt to treat risks to which their information systems are exposed.

4.3.3.4. Treating the risk

The purpose of treating or controlling a risk is to reduce, if not totally eliminate the adverse impacts of the known or perceived risks inherent in a particular undertaking, even before any damage or disaster takes place (Gundlach, 2011). Treating risks occurs when an organisation proactively takes measures to reduce the vulnerability of an asset to successful exploitations of vulnerabilities in it (Navarro, 2001). This strategy enables the activity or action to continue within the organisation, but action is available to reduce the risk to an accepted level (Elky, 2006). Mitigation of risks often requires management to select appropriate security controls, procedures or mechanisms to either prevent a risk from occurring or detect a risk before or after it has occurred (Dorian, 2012). Most of the information security controls are technical in nature and include hardware and software tools that restrict access to buildings, rooms, computer systems and programs in order to prevent improper use (Sveen, Torres and Sarriegi, 2009). Some of these security controls are too technical or expensive to be implemented in small-scale organisations with already stretched human and financial resources as a result alternative affordable security controls have to be used.

There are four different types of security controls commonly used in risk treatment, namely detective, preventive, corrective and directive (Rainer *et al.* 1991; Consultative Objective and Bi-functional Risk Analysis COBRA, 2005; O'Donnell & Best, 2005; Elky, 2006; Metras, 2008; Gundlack, 2011; Dorian, 2012).

- **Detective security controls** identify and characterise an incident while in progress and alert the system user or security system about the intruder during an event or process (Rainer *et al*. 1991; Metras, 2008; Dorian, 2012). Detective security controls are designed to identify unfavourable events after they have occurred (TSQ, 2011). Intrusion detection security controls in intrusion detection systems are popular examples (COBRA, 2005; Elky, 2006; Sveen *et al*. 2009). These security controls are only appropriate when it is possible to accept the loss or damage incurred. In such a situation, an organisation is likely to lose reputation. In the context of secondary schools, fraud can be detected after it has occurred or detect marks alterations after learners have been promoted to other grades.

- **Preventive security controls** are designed to limit the possibility of an undesirable outcome being realised (Elky, 2006; Sveen *et al*. 2009; TSQ, 2011). These security controls are intended to prevent an incident from occurring. This is achieved by locking out unauthorized intruders, separation of duty, installing security cameras to deter criminal activity (Dorian, 2012; TSQ, 2011). These strategies can be implemented in secondary schools but have financial implications to these organisations.

- **Corrective security controls** are mechanisms designed to correct undesirable outcomes which have been realised (Rainer *et al*. 1991; Sveen, et.al., 2009; TSQ, 2011). Examples of corrective security controls include rotating staff positions, internal audit review of preventative and detective controls, or a change to management procedures (Elky, 2006). After the event, corrective controls limit the extent of any damage caused by the incident by recovering the organisation to normal working status as efficiently as possible. These controls are suitable for secondary schools in the event that an attack occurs unexpectedly.

- **Directive (deterrent) security controls** are designed to ensure that a particular outcome is achieved (Elky, 2006; Gundlack, 2011; TSQ, 2011). They are particularly important when it is critical that an undesirable event be avoided, particularly in critical information systems. Figure 4.2 shows threat-attack-risk security controls.

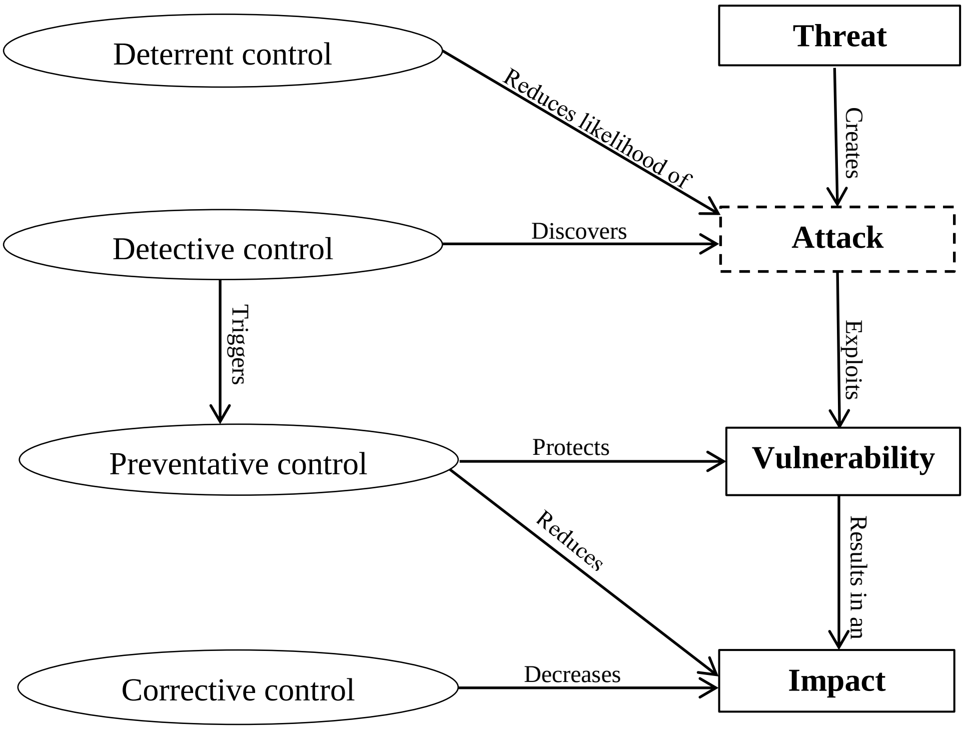


Figure 4.2: List of security controls and how they relate to attacks: Source: COBRA (2005)

The major purpose of risk treatment strategies is to reduce the risk level of unacceptable risks to an acceptable level or the target risk level (ACTIA, 2004). This means that management has to define criteria for describing acceptable levels of risks for their organisations. This could be difficult for secondary schools due to lack of expertise pertaining to CISs. However, the risk controls in a computerised information system can be used as a guide to the acceptable risk level that the management in each school expects. This study seeks to establish what controls are in place for risks identified in secondary schools, and this will be done in Chapter 7. Once risks have been assessed there is a need to consult other members of the organisation who use the same information systems to communicate the outcome of the risk assessment so that collective decision will be taken on how to treat risks.

4.3.4. Communication and Consult

Successful risk management relies on communication with all stakeholders in order to improve the level of understanding and treating risks. Risk communication involves an interactive dialogue between users and risk assessors and risk managers which actively informs the other processes (Meek, 2005). In this study information on risks and control measures identified by the risk assessment and analysis process will be communicated using appropriate copies of risk assessments available to management and all the CISs users concerned.

4.3.5. Monitor and Review

Effective risk management requires a reporting and review structure to ensure that risks are effectively identified and assessed and that appropriate controls and responses are in place (The Association of Insurance and Risk Managers AIRMIC, The National Forum for Risk Management ALARM and The Institute of Risk Management IRM, 2002). This step ensures that an organisation’s risk management programme remains relevant and all input data, including likelihood and consequence, are up-to-date. Based on the AS/NZS ISO 31000:2009, the monitoring and reviewing relates to all of the five elements of the risk management workflow. The importance of the monitoring and review process is to provide assurance that there are appropriate controls in place for the organisation’s activities and that the procedures are understood and followed (AIRMIC, ALARM & IRM, 2002). Furthermore, risk monitoring and review ensure that the responses are performing adequately throughout the life cycle of the system, facility or activity (Campbell, 2008). Monitoring and review exercises depend on audits or the results of previous analyses and evaluations which secondary schools involved in this study might hardly have. The monitoring and review process is essential in determining whether:

- the measures adopted result in what was intended (AIRMIC *et al.* 2002; Elky, 2006);
- the procedures adopted and information gathered for undertaking the assessment were appropriate (AIRMIC *et al.* 2002; Elky, 2006); and
- improved knowledge would have helped to reach better decisions and identify what lessons could be learnt for future assessments and management of risks (AIRMIC *et al.* 2002; Elky, 2006);

In schools, users of CISs should be given responsibility to oversee the process and develop reporting procedures, discussing and helping to implement solutions, as well as monitoring the solutions for effectiveness. This is likely to help in monitoring and reviewing the effectiveness of the control measures on an on-going basis.

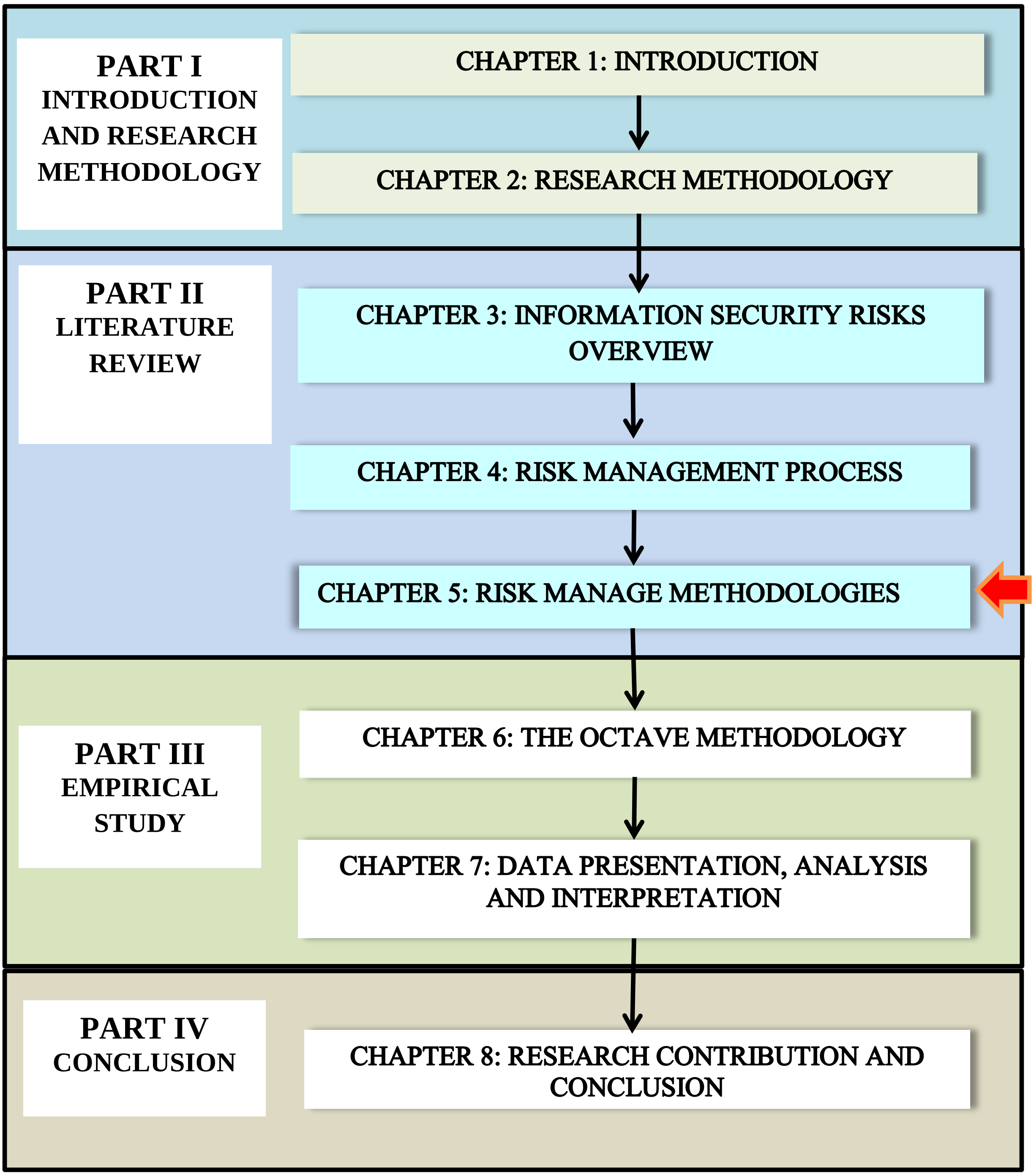
4.4. CONCLUSION

CISs are always exposed to a variety of risks which could be identified by carrying out a risk management exercise. Risk management is an on-going systematic process that helps an organisation to identify, analyse, assess, evaluate, track and communicate risks in its information system assets, to enable the management to put security controls in place to reduce the loss due to threat attacks. Risk management implemented by an organisation depends on a risk management framework that an organisation chooses. The AS/NZS ISO 31000:2009 is a very popular framework that an be used to understand risk assessment and analysis method. The AS/NZS ISO 31000:2009 risk management framework has been depicted as comprising three interacting components; the workflow, monitor and review, and communicate and consult. When this framework is adopted, three major tasks are performed; establishing the context, assessing risks and treating risks. Risk assessment has been discussed taking into account its importance in this whole process. Risk analysis has also been identified as an important aspect of risk assessment. A number of risk treatment and control options have been discussed. Issues arising from these control measures have also been discussed. The discussions have been left open for further exploration depending on the risk assessment and analysis methodologies to be used.

This study uses a qualitative risk management methodology, namely the OCTAVE-small methodology as discussed in chapters 5 and 6. The next chapter, Chapter 5 elaborates on risk assessment and analysis methodologies in general.

CHAPTER 5

5. RISK MANAGEMENT METHODOLOGIES


PART I
INTRODUCTION AND RESEARCH METHODOLOGY
CHAPTER 1: INTRODUCTION
CHAPTER 2: RESEARCH METHODOLOGY
PART II
LITERATURE REVIEW
CHAPTER 3: INFORMATION SECURITY RISKS OVERVIEW
CHAPTER 4: RISK MANAGEMENT PROCESS
CHAPTER 5: RISK MANAGE METHODOLOGIES
PART III
EMPIRICAL STUDY
CHAPTER 6: THE OCTAVE METHODOLOGY
CHAPTER 7: DATA PRESENTATION, ANALYSIS AND INTERPRETATION
PART IV
CONCLUSION
CHAPTER 8: RESEARCH CONTRIBUTION AND CONCLUSION

5.1. INTRODUCTION

Information security risk management is generally viewed as a highly technical process that may require expensive equipment and specialist assistance (Kite, 2009). On many occasions small-scale organisations tend to use common sense in risk management or even abandon the practice altogether (Panda, 2009). Risk management leads to the understanding of the risks to which CISs could be exposed to. There are various risk management methods and tools from which an organisation can possibly choose depending on expertise at its disposal. These methods are categorised as quantitative and qualitative respectively.

Chapter 2 discussed the research methodology for this study, which is a qualitative case study based on the interpretive paradigm; Chapter 3 outlined information security risks and Chapter 4 explored a risk management framework. In order to implement data generating techniques, this study has to utilise a particular risk assessment and analysis technique. The main purpose of this chapter is to discuss risk assessment and analysis techniques justifying the choice of the qualitative methodology used in this research study. Important aspects regarding qualitative risk assessment and analysis methods are exemplified by the Operationally Critical Threat, Asset and Vulnerability Evaluation method. For each discussed method, advantages and disadvantages are given and contextualised to the school situation.

The structure of this chapter includes an introduction, a discussion of risk management methods as quantitative and qualitative and the conclusion.

5.2. QUANTITATIVE METHODS

Quantitative risk management methods used in information systems are derived from risk methodologies used by financial institutions and insurance companies (Elky, 2006). These methods use mathematical and statistical tools in an attempt to assign specific numbers to the costs of controls and the amount of damage that can take place to an organisation’s assets (Nosworthy, 2000; Lo & Chen, 2012). An organisation opts to use a lot of time in developing complex mathematical models to achieve an acceptable level of risk by physically calculating the threat frequency and the likelihood of occurrence (Nosworthy, 2000). To achieve this, values are assigned to information systems assets, business processes, recovery costs and impact. These methods, therefore, measure risk in terms of direct and indirect costs (Elky, 2006). Quantitative risk management methods require a large amount of preliminary work to collect precise values of all elements, including asset values, threat frequency, control effectiveness, and control costs (Lo & Chen, 2012). These risk assessment and analysis methods consider information systems risk exposure as a function of the probability of a threat and the expected loss due to the vulnerability of the organisation to this threat (Nosworthy, 2000; Feng & Li, 2011). When an organisation decides to use a quantitative method, individuals involved in the risk assessment and analysis process ought to reach consensus regarding the value of information technology assets and probability estimates (Rainer *et al*. 1991).

Popular examples of quantitative risk assessment and analysis methods are Annualised Loss Expectancy (ALE), Courtney's method, Livermore Risk Analysis Methodology (LRAM), and Stochastic Dominance (Rainer *et al*. 1991; Hoo, 2000; Elky, 2006; Beachboard *et al*. 2008). The basis of these quantitative methods is on regarding loss exposure as a function of the vulnerability of an asset to a threat multiplied by the probability of the threat becoming a reality. To illustrate how quantitative methods are used, the ALE method is chosen as an example because it looks less intimidating than other quantitative methods.

When the Annualised Loss Expectancy (ALE) is used, the initial step is listing all information systems or information technology assets (Hoo, 2000). Potential threats to those assets are analysed along with the loss that would result from the realisation of those threats (Rainer *et al*. 1991; Beachboard *et al*. 2008). Each asset’s vulnerability to a threat is expressed as a probability of occurrence per year. The expected loss per year from a particular threat/vulnerability pair is obtained by multiplying the probability of occurrence per year by the expected loss (Rainer *et al*. 1991; Elky 2006). The sum of all individual asset expected losses represents the total information systems security risk exposure. This is the figure which management use to make a decision to spend for security and preventive measures if necessary. This complex process is carried out by experts from within or outside the organisation. The Annualised Loss Expectancy model is represented by the formula below.

$$\textbf{Total information technology risk exposure} = \sum_{i=1}^{n} (\mathbf{V}\text{i} + \mathbf{EL}\text{i})$$

Where vulnerability = V_i = probability of occurrence per year, and expected loss = EL_i = expected loss of ith threat/vulnerability pair.

Quantitative risk assessment and analysis methods can provide a measurement of the risk impacts' magnitude that can be used in the cost-benefit analysis of recommended controls (Stoneburner *et al*. 2002). This makes these methods more advantageous over qualitative ones. Mathematical formulae used in these methods are easily verifiable and makes the methods to be viewed as being objective (Rainer *et al*. 1991; Lo & Chen, 2012). Therefore, an organisation that decides to use quantitative methods capitalises on this objectivity in risk assessment and analysis (Karabacaka & Sogukpinar, 2003). Besides objectivity of quantitative risk assessment methods, Meek (2005) argues that these methods are assessor independent, compatible with statistical interrogation, allow comparisons of risk assessment and analysis results; and allow formal incorporation of some types of uncertainty. If schools had expertise in risk management, they could possibly benefit from these methods.

The success of quantitative methods depends heavily on the availability of good and reliable data for the analysis, which is very hard to obtain (Thiagarajan, 2003; Beachboard *et al*. 2008; Tiwari, 2010). Lack of good quality data used in estimating probabilities of occurrence or loss expectancies is a big problem when the assessments are performed (Lo & Chen, 2012). Performing a quantitative risk assessment and analysis for information technology-based information systems is not cost-effective for two reasons: the difficulties in identifying and assigning a value to existing assets, and lack of statistical information that would make it possible to determine frequency of occurrence of attacks on information systems (Elky, 2006). The disadvantage of quantitative methods is that of depending on the numerical ranges used to express the measurement which may result to distorted or unclear meaning of the quantitative risk assessment and analysis outcome (Stoneburner *et al*. 2002).

Confronted with this situation, an organisation which chooses to conduct risk assessment and analysis using quantitative methods has to overcome numerous difficulties. From the onset, identifying all possible relevant threats and reliably estimating the probability of occurrences would prove to be extremely difficult if not impossible (Ding, 2002; Beachboard *et al*. 2008; Katsikasa, 2009). The process of estimating costs associated with different types of system failures or compromises is also an inexact process that gives rise to inaccuracies in the final calculations of asset exposures to the risks (Karabacaka & Sogukpinar, 2003).

Therefore, it is clear that the choice of risk management method depends on the understanding and appropriate application of that method in a given organisational context. The latter represents a daunting task particularly to resource and expertise constrained small and medium-sized enterprises (Beachboard *et al*. 2008). This situation is even worse in secondary schools where personnel with baseline computing skills are only concerned with the use of CISs regardless of the perennial security risks associated with these information systems assets.

Coupled with this is the issue of financial constraint that has to be overcome by these organisations. Risk assessment and analysis conducted using quantitative methods are generally more expensive and demand greater experience and advanced tools than those conducted using qualitative methods (Rot, 2008). Therefore, this researcher advocates the use of qualitative risk assessment and analysis methods for secondary schools' CISs, discussed in the next section.

5.3. QUALITATIVE METHODS

Research indicates that most of the quantitative risk assessment and analysis techniques are either too difficult to understand or use by small-scale organisations (Alberts & Dorofee, 2001). Subsequently, these organisations may resort to unsanctioned methods or avoid carrying out a risk management exercise completely (Beachboard *et al*. 2008). Therefore, small-scale organisations require simple and participatory risk assessment and analysis methods mostly in the qualitative category.

Qualitative risk assessment and analysis assume that there is already a great degree of uncertainty in the likelihood and impact values and defines them in subjective or qualitative terms (Elky, 2006). Since qualitative methods depend to a great extent on the analyst's experience, the process and the results of the security risk assessment are relatively subjective in nature (Feng & Li, 2011). A qualitative risk management method also indicates a more subjective approach in which the threats are given a ranking of none/low, medium, high or very high mainly based on the knowledge and judgement of those doing the analysis (Nosworthy, 2000). When a qualitative method is used, the probability data are not required, only the estimated potential loss is used (Feng and Li, 2011). In contrast to quantitative risk assessment methods, qualitative risk assessment methods are based on judgment, intuition and experience of the team that conducts this exercise (Lo & Chen, 2012). This makes qualitative risk assessment and analysis methods suitable for use in secondary schools where there is no expertise in risk management. There is a high possibility that when school managers and CISs users develop a culture of risk management, they may explore other risk management methods.

Qualitative risk management methods determine the impact and likelihood of the identified risks in a rapid and cost-effective manner than the quantitative methods (Rainer *et al*. 1999; Elyse, 2007). These methods assess the effects of the identified risk factors, creating priorities that can be used to decide on how to solve the potential risk, depending on the impact they could have on the information systems (Mazareanu, 2007). Most qualitative methods are simple and easy to use with less technical people in any organisations (Panda, 2009). Qualitative methods express risks in terms of descriptive variables or adjectives instead of precise monetary terms, therefore, requiring less time, finance and effort to implement (Rainer *et al*. 1999; Karabacaka & Sogukpinar, 2003). This makes them simple because they utilise the language which non-technical people are familiar with. Therefore, qualitative risk assessment and analysis methods are a better choice for use in schools where there are no risk management personnel.

A risk matrix is normally used when a qualitative risk assessment method is implemented (Elky, 2006; Renfroe & Smith, 2011). A risk matrix is a combination of the impact of loss rating and the vulnerability rating qualitatively determined by risk assessors (Renfroe & Smith, 2011). The vulnerability to threat are ranked as very high, high, moderate or low while the impact of loss is ranked as devastating, severe, noticeable or minor. Table 5.1 shows a possible matrix used for identifying risk levels when a qualitative method is used.

Table 5.1: Matrix Identifying levels of risks

		Vulnerability to threat			
		Very High	High	Moderate	Low/None
Impact of loss	Devastating	H	H	H	H
	Severe	H	H	M	M
	Noticeable	H	M	M	L
	Minor	M	M	L	L

Source: Elky (2006) and Renfroe and Smith (2011)

Explanations on Table 5.2 are used to interpret the ratings in the matrix on Table 5.1

Table 5.2: Interpretation of the risk ratings

H	High risks that need immediate implementation of recommended security risk controls to mitigate these risks
M	Moderate risks where control implementation should be planned in the near future.
L	Low risks in which control implementation will enhance security, but is of less urgency than the above risks.

Source: Elky (2006) and Renfroe and Smith (2011)

These qualitative measures can easily be understood compared to the quantitative ones. These measures also bring about some standardised guidelines to regulate the manner in which different users will use the qualitative tools.

A number of qualitative risk management techniques can pose serious problems in secondary schools due to a number of glitches associated with them. The Hazard And Operability study (HAZOP), Failure Mode and Effects Analysis (FMEA) or Failure Mode and Effects Criticality Analysis (FMECA) and Central Computer and Telecommunications Agency Risk Analysis and Management Method (CRAMM) either require highly trained technical teams to perform risk assessment and analysis, labour intensive or strong financial bases (Lander, 2004; Mraz & Huber, 2005; Rausand, 2005; Rot, 2008). Secondary schools hardly have such expertise and financial bases. This makes the use of these methods unsuitable by secondary schools. However, not all qualitative risk assessment and analysis techniques require highly technical people or strong financial support. The OCTAVE method provides an easy, cheap and viable means of achieving the same objectives that any of the other methods is capable of.

The Operationally Critical Threat, Asset and Vulnerability Evaluation risk management technique is concerned with all risk components that include assets, threats and vulnerabilities (Alberts & Dorofee, 2001). OCTAVE is a comprehensive method to assess and analyse information security risks based on information technology asset type and is ideal to be used by internal organisation resources to perform threat/technology risk assessment and analysis (Storms, 2003). A number of studies on OCTAVE as an information security risk management technique cite the merits of using this technique in organisations of different sizes regardless of the technical skills the personnel have (Panda, 2009). One important benefit of OCTAVE is that it is participatory and self-directed (Pyka & Januszkiewicz, 2006; Panda, 2009). When this technique is used, different stakeholders have a chance to actively get involved in the risk assessment and analysis activities, thereby improving their decision making process concerning the protection and management of information systems resources (Pyka & Januszkiewicz, 2006).

Qualitative risk management methods have their own disadvantages such as being inexact and subjective (Rainer *et al*. 1999; Karabacaka & Sogukpinar, 2003). Furthermore, lack of specific quantifiable measurements of the magnitude of the impacts, makes a cost-benefit analysis of any recommended controls difficult when qualitative risk management methods are used (Stoneburner *et al*. 2002). However, Elky (2006) and Elyse (2007) suggest that the use of unbiased and accurate data can improve the credibility of the outcome of a qualitatively conducted risk assessment and analysis exercise. Rot (2008) summarises the advantages and disadvantages of quantitative and qualitative risk assessment and analysis techniques as shown on Table 5.3 below.

Table 5.3 below indicates that qualitative risk management methods have more advantages than quantitative methods. Qualitative methods also have fewer disadvantages than quantitative methods. Their simplistic, easy to use, time saving and financial sustainability makes them potentially viable for small-scale organisations. Regardless of the cited demerits of qualitative methods in general, this study finds it plausible to implement the

OCTAVE risk assessment and analysis technique. A detailed discussion of the OCTAVE method is presented in Chapter 6.

Table 5.3: Advantages and disadvantages of quantitative and qualitative methods of risk assessment and analysis

Item	Quantitative methods	Qualitative methods
Advantages	• They cater for the definition of consequences of incidents occurrence quantitatively which facilitates the realisation of cost benefits analysis during the selection of protection strategies • They give a more accurate image of risk.	• Allow ordering of risks according to priority. • Allow determination of areas of greater risk in a short period of time • Can be conducted in shorter time and with less expenditure • Analysis is relatively easy and cheap.
Disadvantages	• Quantitative measures depend on the scope and accuracy of defining measurement scale. • Results of analysis may be not precise and even confusing. • Normal methods must be enriched in qualitative description (in the form of comments, interpretations). • Analysis conducted by application of those methods is generally more expensive, demanding greater experience and advanced tools.	• It does not allow for determination of probabilities and results using numerical measures. • Costs-benefits analysis is more difficult during the selection of protections. • Achieved results have general character.

Source: Rot (2008)

5.4. CONCLUSION

This chapter discussed risk management methodologies justifying the selection of the OCTAVE-small method derived from qualitative methods. The choice of a risk management method for this study was influenced by a number of factors such as the unavailability of risk management personnel, finance, types of risks and size of organisation concerned. Quantitative and qualitative risk assessment and analysis methods have been used in other projects to solve information security risks. It has been illustrated that each category of methods has its own advantages and disadvantages. Quantitative methodologies are objective and verifiable due to the use of mathematical formulae. Besides complexities, quantitative methods are also expensive for small-scale organisations that have constrained budgets. Only organisations with experts in risk management may implement them. Therefore, using quantitative methods in schools is not cost effective. Qualitative risk assessment and analysis methods provide a rapid and cheaper alternative to quantitative methods. However, some of the qualitative methods are as difficult as quantitative for use in high schools where there are scarce information security personnel. After weighing selected qualitative methods, this research study justifiably selected the OCTAVE risk management method. The OCTAVE method provides an alternative from which different organisations depending on the experience of the personnel they have could possibly conduct a risk assessment and analysis exercise. Unlike quantitative methods, qualitative methods are criticised for being too subjective and difficult to verify their results.

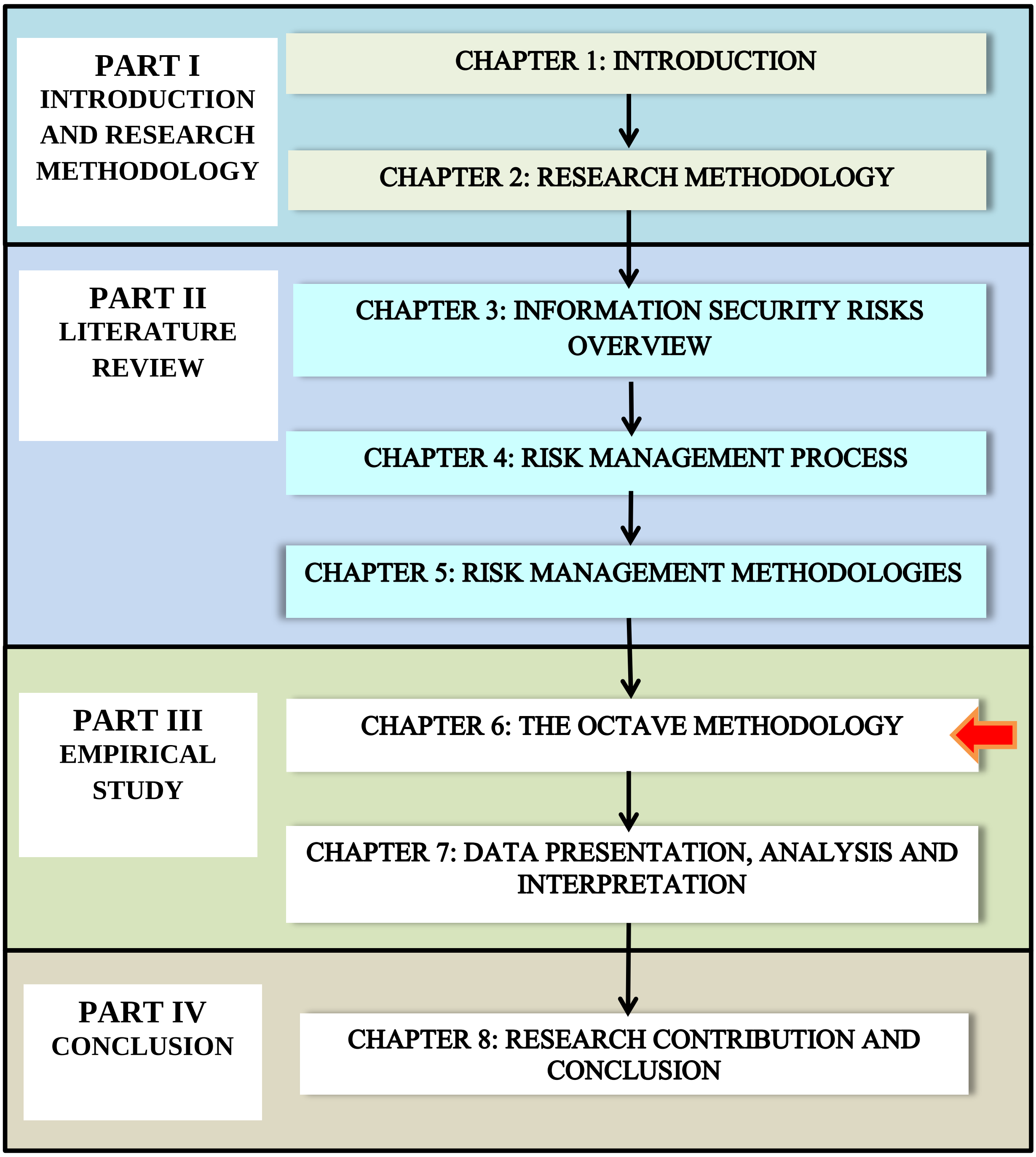
Having selected the risk management method for this study, effort is directed at describing that method and how it would be used in this study. Chapter 6 explores the OCTAVE risk assessment and analysis method and how one of its variants, OCTAVE-small will be used in this research study.

PART III

EMPIRICAL STUDY

CHAPTER 6

6. THE OCTAVE-SMALL METHODOLOGY


PART I
INTRODUCTION AND RESEARCH METHODOLOGY
CHAPTER 1: INTRODUCTION
CHAPTER 2: RESEARCH METHODOLOGY
PART II
LITERATURE REVIEW
CHAPTER 3: INFORMATION SECURITY RISKS OVERVIEW
CHAPTER 4: RISK MANAGEMENT PROCESS
CHAPTER 5: RISK MANAGEMENT METHODOLOGIES
PART III
EMPIRICAL STUDY
CHAPTER 6: THE OCTAVE METHODOLOGY
CHAPTER 7: DATA PRESENTATION, ANALYSIS AND INTERPRETATION
PART IV
CONCLUSION
CHAPTER 8: RESEARCH CONTRIBUTION AND CONCLUSION

6.1. INTRODUCTION

Organisations that are concerned about their information assets security explore and examine various risk management methods to ensure that they provide adequate security to their information systems (Storms, 2003). Some information security risk management methods tend to be incomplete, expert-driven or both (Panda, 2009), making them difficult and inappropriate to implement with small-scale organisations (Alberts & Dorofee, 2003; Beachboard *et al*. 2008). In large commercial organisations there are teams of experts for information security risk management while small-scale organisations like secondary schools hardly have the capacity to do so. Small-scale organisations require user friendly information security risk management methods that can be implemented by a team or an individual from within the same organisations. The Operationally Critical Threats, Assets and Vulnerability Evaluation is designed to meet this end (Woody, Coleman, Fancher, Myers & Young, 2006). This study utilises the OCTAVE risk assessment and analysis method to study CISs in two selected secondary schools.

Chapter 5 dealt with quantitative and qualitative risk assessment and analysis techniques in which the use of a qualitative method in this study was justified. The OCTAVE risk assessment and analysis method was indicated as the most viable method for this study. Therefore, the purpose of this chapter is to elaborate on the OCTAVE risk assessment and analysis method, outlining its components and how it will be applied in this research study. The chapter also describes how data collection methods discussed in Chapter 2 and Chapter 4 were applied with the OCTAVE technique.

The structure of the chapter is as follows: a brief introduction, definition of OCTAVE, key features and different types of OCTAVE, the application of OCTAVE-small to this research, and finally the conclusion.

6.2. WHAT IS OCTAVE?

Operationally Critical Threats, Assets and Vulnerability Evaluation is a qualitative risk-based strategic assessment and planning method for information security (Panda, 2009). It is a process-driven methodology to identify, prioritise and manage information security risks (Alberts & Dorofee, 2004). OCTAVE is a collection of techniques and tools for identifying and managing information security risks (Alberts, Behrens, Pethia & Wilson, 1999). Accordingly, OCTAVE is a comprehensive evaluation method that allows an organisation to identify the information assets that are important to its mission, the threats to those assets, and the vulnerabilities that may expose those assets to the threats (Panda, 2009). This is the specific objective of this research study.

In general, the OCTAVE method is designed to provide complete information for information security risk management (Alberts & Dorofee, 2001). OCTAVE includes all components of risk (assets, threats, and vulnerabilities) and as a result an organisation gets sufficient data to fully match its information security risk protection strategy unlike conventional methods (Alberts & Dorofee, 2001; Panda, 2009). This implies that OCTAVE is a risk assessment and analysis method driven by operational risk and security practices where information technology is examined only in relation to the information security practices (Sosonkin, 2005).

Unlike other risk management approaches that highlight technological risk only, and also led by experts who evaluate systems, OCTAVE focuses on security practice, it is self-directed, and stresses on organisation-wide strategic issues. Table 6.1 shows a comparison of the OCTAVE method and other risk assessment methods (Alberts & Dorofee, 2001; Sosonkin, 2005)

Table 6.1: Comparison of OCTAVE and other risk assessment methods

OCTAVE	OTHER EVALUATIONS
Organisation evaluation	System evaluation
Focus on security practices	Focus on technology
Strategic issues	Tactical issues
Self-direction	Expert led

OCTAVE also defines assets as including people, hardware, software, information and systems (Violino, 2010).

6.3. OCTAVE AS A FUNCTIONAL METHOD

Risk assessment and analysis methods are classified as temporal, comparative or functional (Campbell & Stamp, 2004; Woody *et al*. 2006). *Temporal methods* focus on technology systems using actual tests, *comparative methods* concentrate on a specific standard and *functional methods* balance the other two by applying tests and standards (Alberts, Dorofee, Stevens & Woody, 2003; Campbell & Stamp, 2004). The OCTAVE method is classified as a functional method whose strength is based on the fact that specific threats, assets, vulnerabilities and controls important to the context of the organisation are included (Alberts *et al*. 2003; Campbell & Stamp, 2004; Woody *et al*. 2006).

A study by Campbell and Stamp (2004) indicates that an organisation can successfully implement a selected risk management programme by balancing two crucial factors namely the knowledge of the method and contextual knowledge. These two factors help to define who should lead the risk management programme in an organisation. From this perspective, experts lead when methodology knowledge is critical, and system owners lead when contextual knowledge is critical (Campbell & Stamp, 2004). Based on this view, OCTAVE is classified as mid-level because it balances the two extremes (Woody *et al*. 2006). This allows some organisations to apply the OCTAVE method unassisted while others enlist specialists to supplement their knowledge of security risk management (Woody *et al*. 2006). This research study seeks to apply the OCTAVE method without assistance from experts but using non-technical personnel; the users of CISs in secondary schools.

Panda (2009) discusses three variants of OCTAVE, namely OCTAVE$^{(SM)}$, OCTAVE-small and OCTAVE-Allegro. OCTAVE$^{(SM)}$ is the original OCTAVE method, which forms the basis for the OCTAVE body of knowledge (Alberts *et al*. 2003; Panda 2009). OCTAVE-small is for small-scale organisations while OCTAVE-Allegro is a streamlined information security risk assessment and analysis methodology suitable for any organisation regardless of its size (Richard, Caralli, Stevens, Young, & Wilson, 2007; Panda, 2009). This study utilises OCTAVE for small-scale organisations (OCTAVE-small) to study secondary schools' CISs. The rationale for choosing OCTAVE-small variant is dealt with in section 6.4 below.

6.4. FEATURES AND BENEFITS OF THE OCTAVE METHOD

There are four basic features of OCTAVE that distinguishes it from other risk assessment and analysis methods namely, self-direction, workshop-based approach, using an analysis or collaborative team and catalogues of information (Alberts & Dorofee, 2001; Pyka & Januszkiewicz, 2006).

Self-direction implies that people from within the same organisation assume responsibility for setting the organisation's security strategy (Woody *et al*. 2006), which is, what this study seeks to attain. An organisation without an in-house capability to perform information security risk assessments and analysis always outsources experts to perform these vital services on its behalf (Alberts *et al*. 1999). The users of information systems in such an organisation are often isolated from the decision-making process and rely mainly on the judgment of external experts (Alberts and Dorofee, 2004). These users do not know the underlying thinking process used by the experts as a result they do not understand or know whether the risk assessment performed for their organisation is adequate (Alberts *et al*. 1999; Alberts & Dorofee, 2001). In such situations, the responsibility is shifted from users to the experts, who are not accountable to the organisation (Alberts and Dorofee, 2001). The OCTAVE-small method can assist an organisation to address such problems. When OCTAVE-small is used, the system users are responsible and accountable as they lead the evaluation and decision making processes (Pyka & Januszkiewicz, 2006). This study utilises a small team of information system users (the collaborative team) to manage the process. This is intended to actively involve the users in the decision-making process (Alberts & Dorofee, 2001).

A **collaborative team is** an interdisciplinary team that comprises of representatives from both the mission-related and information technology areas of an organisation (Alberts & Dorofee, 2001). This team performs a number of OCTAVE activities such as risk identification, analysis and evaluation (Alberts & Dorofee, 2001; Panda, 2009). The size of the collaborative team is determined by the size of the organisation and the scope of evaluation (Woody *et al*. 2006). This study is based on secondary schools whose employees are less than eighty and the computing facilities are run by single-small departments that include mission related personnel. In such cases, Alberts *et al*. (2003), Sosonkin (2005) and Pyka & Januszkiewicz (2006) suggest the use of a team of between three and five people, preferably the users of the information systems.

Alberts and Dorofee (2001), Sosonkin (2005) and (Panda 2009) provide basic tasks that the OCTAVE-small collaborative team should achieve as:

- identifying critical information assets;
- identifying the organisation's information security risks;
- focusing risk analysis activities on identified critical assets;
- gathering any supporting data that are necessary;
- analysing threat and risk information to determine priorities;
- developing a protection strategy for the organisation;
- developing mitigation plans to address the risks to the organisation's critical assets;

OCTAVE uses a **workshop-based approach** for gathering information and making decisions **(**Alberts and Dorofee, 2001; Sosonkin, 2005; Panda, 2009). This is done through Phases 1 to 3 in OCTAVE $^{(SM)}$ and Processes 1 to 4 in OCTAVE-small. Each activity provides key information for the whole process. OCTAVE also relies upon the c**atalogues of information** namely:

- *catalogue of practices* - a collection of good strategic and operational security practices (Alberts & Dorofee, 2001; Sosonkin, 2005)
- *threat profile* - the range of threats that an organisation needs to consider (Alberts & Dorofee, 2001; Sosonkin, 2005)
- *catalogue of vulnerabilities* - a collection of vulnerabilities based on platform and application (Alberts & Dorofee, 2001; Sosonkin, 2005)

An organisation using OCTAVE compares itself against these catalogues of information in order to define all the essential components of information security risk assessment (Alberts *et al*. 1999; Sosonkin, 2005). This further enables an organisation to make information-protection decisions based on risks to the confidentiality, integrity and availability of its critical information assets (Sosonkin, 2005; Panda, 2009). OCTAVE gives an organisation a comprehensive, systematic, context-driven approach to manage its information security risks (Pyka & Januszkiewicz, 2006).

The benefits of using OCTAVE-small are:

- **self-directedness - s**mall teams of organisational personnel from different departments and information technology work together to address the security needs of the organisation (Alberts & Dorofee, 2001; Pyka & Januszkiewicz, 2006);
- **flexibility** - each OCTAVE method is tailored to the organisation's unique risk environment, security and resiliency objectives, and skill level (Sosonkin, 2005; Pyka & Januszkiewicz, 2006; Panda 2009). This study adopts OCTAVE-small tailored for small to medium-scale organisations, thus justifies its use in secondary schools, one of the objectives of this research study;
- **evolving** – OCTAVE-small advances an organisation toward an operational risk-based view of security and addresses technology in a business context (Sosonkin, 2005; Pyka & Januszkiewicz, 2006; Panda, 2009).

6.5. JUSTIFICATION FOR THE USE OF OCTAVE-SMALL

The size and layering of an organisation’s computerised information system is a major determinant in choosing the type of OCTAVE method for a particular organisation (Panda, 2009). A large and multi-layered hierarchical organisation that has sections which maintain their own information technology infrastructure and employees above eighty adopts OCTAVE$^{(SM)}$ (Siu, 2007; Panda, 2009). A small organisation with flat-layered hierarchical structure and employs less than eighty is recommended to use OCTAVE for small-scale organisations (OCTAVE-small) (Alberts & Dorofee, 2002; Sosonkin, 2005) or OCTAVE Allegro. OCTAVE-small is suitable for small-scale organisations such as secondary schools because it is less complex than OCTAVE$^{(SM)}$ and can be implemented by users who are not experts in risk management.

The fact that OCTAVE-small approach uses an asset-based information security risk assessment means that information security risk is carefully considered based on the organisational and technological vulnerabilities that threaten a group of mission-critical assets (Woody *et al*. 2006). In order to attain the objectives of this study, OCTAVE-small will provide answers to these questions:

- What critical information systems assets do secondary schools have?
- What critical information assets in secondary schools require protection?
- What threats or vulnerabilities are the school CISs assets be protected against?
- What is the level of information security breaches in these CISs assets?

- What level of protection is needed to mitigate risks?
- What is the impact on CISs if the existing protection fails?

Answering these questions assists the researcher to gather full sets of data that could possibly match mitigation strategies to their information security risks. This could also enable management to decide on information protection based on risks to the confidentiality, integrity and availability of critical information assets (Panda, 2009).

Table 6.2 is a list of questions which were used to assist the researcher to decide whether to or not to use OCTAVE-small in this study as suggested by Alberts and Dorofee (2003).

Table 6.2: Check-list for the applicability of OCTAVE-small to this study

	Item	**Choice**	
		Yes	No
1.	Is the organisation being studied small?	√	
2.	Does the organisation have a flat or simple hierarchical structure?	√	
3.	Is there a group of three to five people who have a broad and deep understanding of the organisation and also possess these skills		
3.1.	*Problem-solving ability*	√	
3.2.	*Analytical ability*	√	
3.3.	*Ability to work in a team*	√	
3.4.	*At least one member with leadership skills*	√	
3.5.	*Ability to spend a few days working on this method*	√	
4.	Do secondary schools outsource all or most of their information technology functions?	√	
5.	Do secondary schools have a relatively simple information technology infrastructure that is well understood by at least one individual in the organisation?	√	
6.	Do secondary schools have limited familiarity with vulnerability evaluation tools within the context of information-related assets or are they unable to obtain the use of this expertise from current service provider to interpret results?	√	
7.	Do secondary schools prefer a highly structured method as opposed to an open-ended method that can be more easily tailored?		√

Source (Alberts & Dorofee, 2003) with modification

An assessment of secondary schools based on this table shows that most of the answers to the questions were YES. This makes OCTAVE-small the most suitable methodology for this study.

6.6. THE OCTAVE-SMALL METHOD

The OCTAVE-small method is a modification of the OCTAVE$^{(SM)}$ approach intended to meet the needs of small and less hierarchical organisations (Panda, 2009). This method is tailored to the more limited means and unique constraints typically found in small-scale organisations (Alberts *et al*. 2003). OCTAVE-small has the same three phases described in the OCTAVE$^{(SM)}$ method but streamlined to four processes instead of the phases (Alberts *et al*. 2003; Panda, 2009). In this study, OCTAVE-small processes were further modified to suit the CISs and level of skills of the personnel in secondary schools. Figure 6.1 is a diagrammatic representation of the OCTAVE-small method.

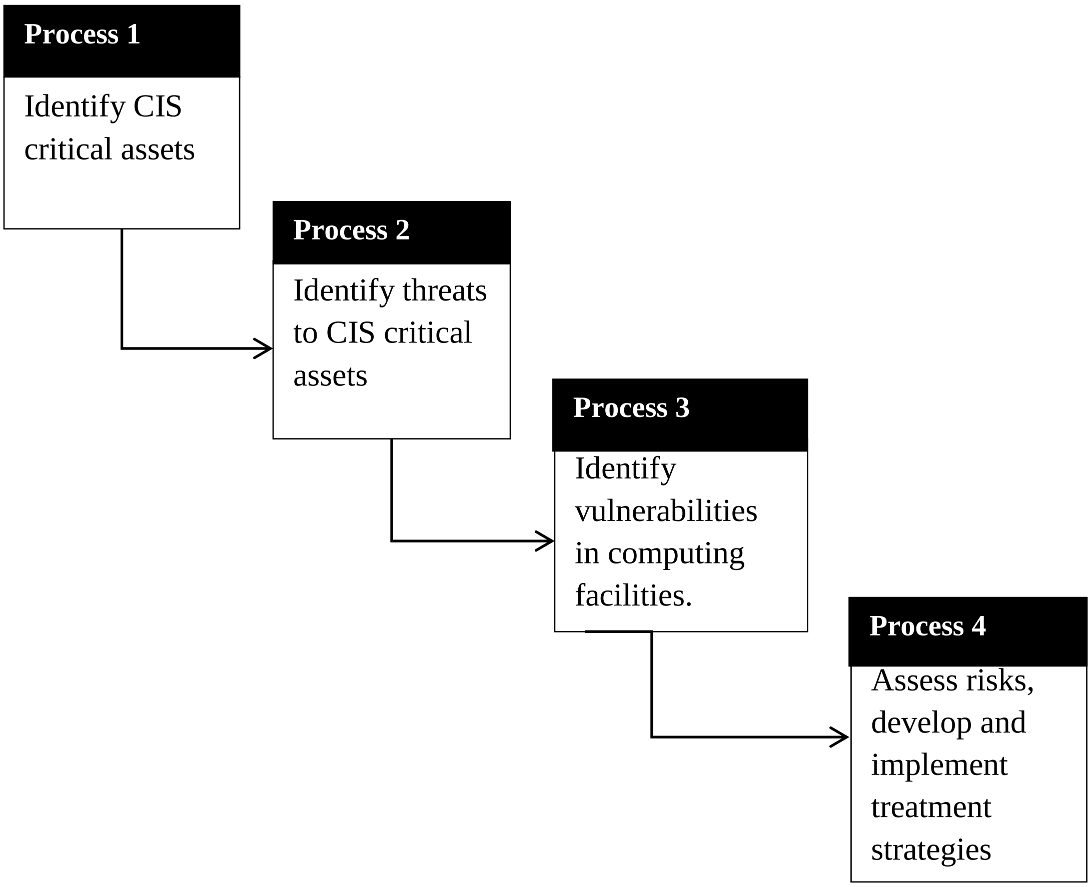

Process 1
Identify CIS critical assets
Process 2
Identify threats to CIS critical assets
Process 3
Identify vulnerabilities in computing facilities.
Process 4
Assess risks, develop and implement treatment strategies

Figure 6.1: The processes of OCTAVE-small

Each OCTAVE-small process is briefly discussed below.

6.6.1. Process 1: Identifying critical organisational information

In this initial step of OCTAVE-small, the collaborative team identifies the organisation's important information-related assets and produces a set of impact evaluation criteria and the current state of the organisation's security practices (Woody *et al*. 2006; Panda, 2009). A list of CISs critical assets will be produced. This study will gather such information from the collaborative team members who are the users of information systems namely the school managers and administrative-educators. This information will be obtained through interviews, observations, inspections and possibly meetings with the users. Information obtained will be used to build asset-based threat profiles described in process 2.

6.6.2. Process 2: Identifying threats to information systems critical assets

The key characteristic of OCTAVE-small is the identification and analysis of threats to the organisation's assets (Alberts and Dorofee, 2001). This process involves an evaluation of organisational aspects in which the information system users from within the organisation contribute their perspectives on what is important to the organisation's information-related assets and what is currently being done to protect those assets. The collaborative team consolidates the information, selects assets that are critical to the organisation, and identifies the threats to these assets (Alberts & Dorofee, 2003). For each identified information asset, collaborative teams define the security requirements and then build a threat profile for each asset (Panda, 2009).

In this study, the collaborative team will build a threat profile by following these three steps suggested by Alberts and Dorofee (2003):

- grouping the information previously obtained from the different users of CISs;
- selecting critical assets; and
- creating a threat profile for each critical asset.

Threat profiles could successfully be built from threat scenarios which are based on known threat sources and their typical threat outcomes and by grouping together threats with a common theme (Storms, 2003). In this study, OCTAVE-small will enable the collaborative team to use the standard categories of threats suggested by Alberts and Dorofee (2001), Storms (2003), Elky (2005) and Panda (2009), listed on Table 6.3 below.

Table 6.3: OCTAVE-small standard threat categories

Threat Category	**Description**
Human actors using network access	These are network-based threats to an organisation’s critical assets. They require direct action by a person and can be deliberate or accidental in nature.
Human actors using physical access	These are physical threats to an organisation’s critical assets. They require direct action by a person and can be deliberate or accidental in nature.
System problems	These threats are problems within an organisation’s information technology systems. For example hardware defects, software defects, unavailability of related enterprise systems, viruses, malicious code
Other problems	These threats are problems or situations that are outside the control of an organisation. For example, natural disasters, such as floods, earthquakes, storms and fire. Such threats could affect an organisation’s information technology systems as well as interdependency risks such as the unavailability of critical infrastructures (telecommunications, electricity). Other types of threats outside the control of an organisation can also be included here. Examples of these threats are power outages or broken water pipes,

Source: Alberts and Dorofee (2001) and Storms (2003)

The collaborative team will also determine whether the resulting outcomes or effects of identified threats lead to:

- disclosure or viewing of sensitive information;
- modification of important or sensitive information;
- destruction or loss of important information, hardware, or software; and
- interruption of access to important information, software, applications, or services.

Alberts and Dorofee (2003) suggest that each category of threats could conveniently be represented as a visual tree structure build around the properties of the identified threat. For example, Figure 6.2 below is a diagrammatic representation of the visual tree structure of category of threats due to actors when using the network to access the critical assets of an organisation. Due to the complexity of OCTAVE-small threat tree diagrams, this study used simple customised tables to build asset threat profiles

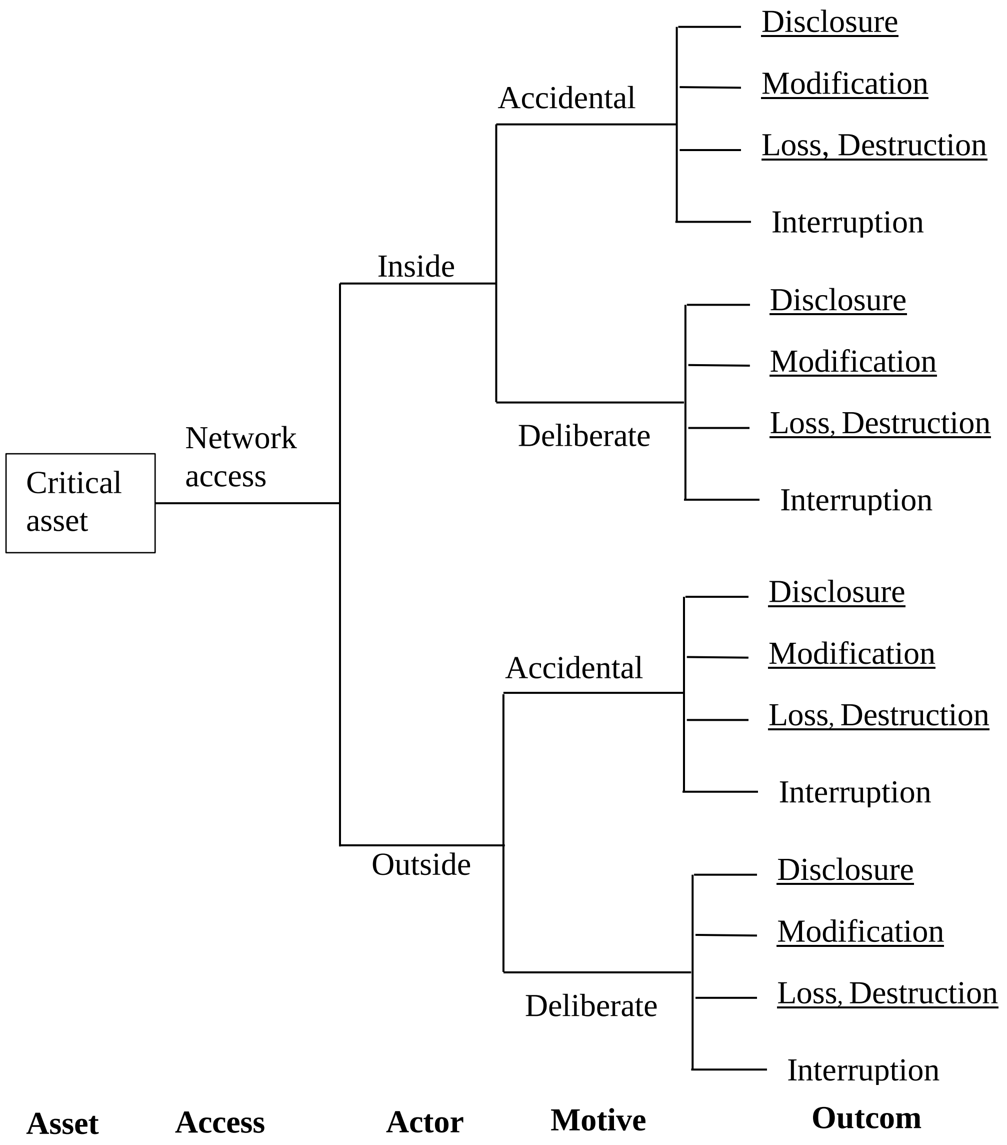


Figure 6.2: Threat profile for critical asset accessed through network

Source: Alberts and Dorofee (2001)

6.6.3. Process 3: Identify infrastructure vulnerabilities

After building threat profiles, the collaborative team concentrates on the computing infrastructure. The main objective is to identify key information technology systems and components related to each critical asset that are part of the computerised information system. The key components are tested for weaknesses (technology vulnerabilities) that could lead to unauthorised action against critical assets (Alberts & Dorofee, 2003). This is a high-level review of infrastructure and technology-related practices done to refine the threat profiles. For example, the collaborative team will analyse the access paths in the systems that support the critical assets and determine how well their technology-related processes are protecting those assets (Woody *et al.* 2006). Physical inspections will be conducted on computer hardware and accessories in order to identify weakness that may be exploited by threats.

6.6.4. Process 4: Conduct risk analysis and develop protection security strategy and mitigation plans

Once infrastructure vulnerabilities are identified, the collaborative team identifies all risks to the organisation's critical assets, analyses them and then decides what action to take. At this point, the team creates a protection strategy for the organisation and mitigation plans to address the risks to the critical assets based upon an analysis of the information gathered. During risk analysis, all identified risks will be qualitatively evaluated for the impact and likelihood of occurring (Alberts & Dorofee, 2003; Panda, 2009). An organisation-wide protection strategy and risk mitigation plans based on security practices will be developed from the evaluation outcomes (Alberts & Dorofee, 2003). Each OCTAVE-small process has its own output as shown on Table 6.4.

Table 6.4: Summary of possible outputs for each OCTAVE-small process

OUTPUT			
Process 1	**Process 2**	**Process 3**	**Process 4**
• Critical assets • Security requirements for critical assets • Areas of concern and impact descriptions • Current security practices	Current threats and vulnerabilities	• Key components for critical assets • Current technological vulnerabilities for key components	• Risk measures • Risks to critical assets • Protection strategies • Mitigation plans

Source: Panda (2009)

Each output on Table 6.4 will be attained after conducting a series of practical activities defined in each OCTAVE-small process. The risk assessment and analysis activities are described in Chapter 7.

In order to perform a risk management exercise using OCTAVE-small method, some preparations should be done before hand. These are explored in section 6.7.

6.7. PREPARATION GUIDELINES

OCTAVE-small provides a module containing all preparation activities that are suggested before starting the risk management programme (Alberts *et al*. 2003).

- ✓ The first and foremost preparation is senior management sponsorship. OCTAVE-small clearly states that senior management sponsorship should be sought prior to the undertaking of the process. This sponsorship is required to encourage staff participation, allocation of resources and support of implementation of the outcomes (van Niekerk, 2005);
- ✓ The selection of the team is the next preparation activity in OCTAVE-small. In this study, the team would be composed of CISs users with skills listed in Table 6.2;
- ✓ Training of at least one team member on OCTAVE-small to create a circular reference, as the creation of the team would already have required some study of the implementation guide (van Niekerk, 2005);

- ✓ Setting the scope of the evaluation to allow the team to identify which areas of the organisation are to be evaluated (van Niekerk, 2005). In this study, CISs was the subset of school units selected for evaluation; and
- ✓ Creating schedule for the activities to be carried out. OCTAVE-small worksheets are provided to offer guidelines of workshop or activity duration, depending on the experience of the team. Table 6.5 shows the duration of the undertaking.

Table 6.5: Duration of OCTAVE-Small

Phase	**From**	**To**
Preparation	4 days	8 days, 4 hours
Build asset-based threat profiles	1 day	2 days, 6 hours
Identify infrastructure vulnerabilities	3 hours	1 day
Develop security strategy and plan	1 day	5 days, 1 hour
Total	**6 days, 4 hours**	**17 days, 3 hours**

Source: Alberts & Dorofee, (2004)

OCTAVE-small risk management is expected to generate data in all its processes using a variety of techniques. Section 6.8 examines the data gathering techniques used in the OCTAVE-small and then link them to those discussed in chapters 2 and 4.

6.8. DATA GENERATING TECHNIQUES FOR OCTAVE-SMALL

Successful implementation of OCTAVE-small requires data for threats, vulnerabilities and exposures of the CISs assets. In this study, the main data collection technique was participatory observation in which the researcher with the help of the collaborative team documented all possible threats, vulnerabilities and exposures in the systems and risk incidents that occurred. This was aided by physical inspections of the CISs and their operational environments. Interviews were conducted with some sampled users of these systems. Chapters 2 and 4 discussed the data collection techniques in detail. A variety of data generating instruments were used in this study, ranging from observation schedule/checklists, inspection checklists and interview schedules. The use of these instruments is dealt with in Chapter 7, which deals with data gathering, the practical component of this research.

The OCTAVE-small risk management method has its weaknesses that need to be overcome during its implementation. Such constraints are briefly discussed in the immediate Section 6.9 below.

6.9. CONSTRAINTS POSED BY OCTAVE-SMALL METHOD

There are a number of constraints associated with the use of OCTAVE-small risk management method. This list exemplifies the constraints.

- OCTAVE-small requires high-quality preparation workshop or meetings (expert knowledge of the business activities) in this case high schools. However, OCTAVE-small is based on the knowledge of employees, rather than on measurements and formal proofs (Bozo & Ruzic 2009; Bozic, 2012).
- OCTAVE-small recommends at least four business units, one of which must be the Information Technology department (van Niekerk, 2005). However, this restriction is questionable, in that many small-scale organisations tend to be made of only one or two business units. In this study, most schools are generally treated as two units namely academic and administrative.
- OCTAVE-small risk assessment may take many workshop or meeting sessions that could prove to be a heavy load and one that most busy organisations would find difficult to accommodate (Jones & Ashenden, 2005). This makes it too difficult to keep the momentum of going in the process if the workshops are spread out over too long a period of time (Jones & Ashenden, 2005). However, OCTAVE-small recognises that the number of workshops held depends on a range of factors, including the scope of the assessment and the resources available for its completion.

Above all OCTAVE-small can be performed either in a workshop-style, collaborative setting or by an individual while being supported by guidance, worksheets and other data generating tools (Stevens, 2005; Richard *et al.* 2007). When OCTAVE-small is implemented in this way, it gives the researcher a leeway to expeditiously carry out the research with minimum problems in the chosen area of study. Furthermore, this helps to place an information security risk assessment within which the organisation can align its processes while ensuring that it follows the principles of OCTAVE-small (Jones &

Ashenden, 2005). Therefore, in this research study, OCTAVE-small was implemented in a collaborative setting that allowed the research to take place in naturalistic settings. This was also intended to give the CISs users a chance to actively participate in the risk management programme.

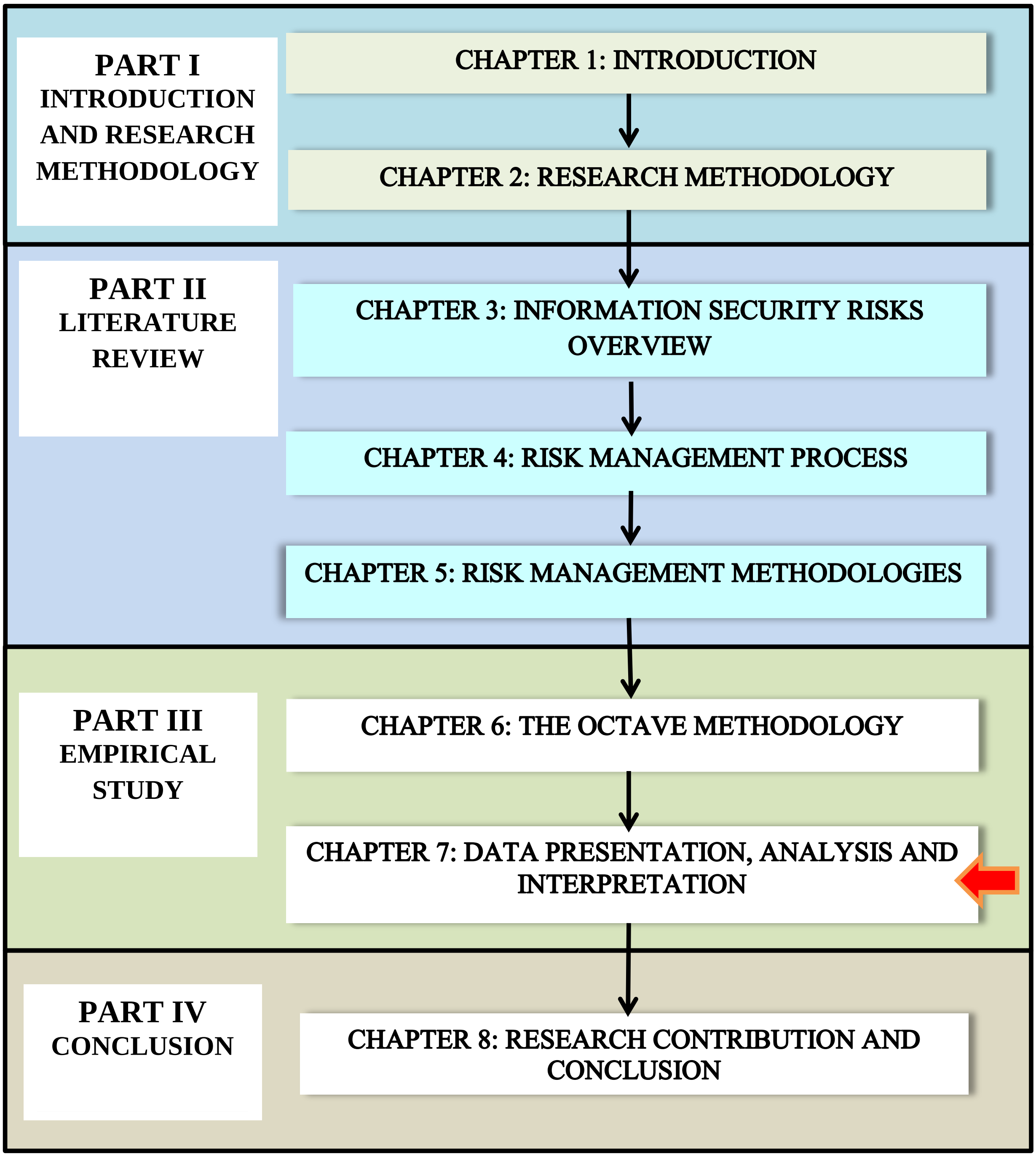
6.10. CONCLUSION

In order to conduct a successful risk management exercise, the most appropriate risk management method was selected from a plethora of the existing methods. A number of factors that influence the choice of such a method were discussed in this chapter. This study implemented OCTAVE-small because it was suitable for flat-layered information systems of an organisation with less than eighty employees. The OCTAVE-small method is a qualitative risk-based strategic assessment and planning method for information security and is a process-driven methodology that identifies, prioritises and manages information security risks. OCTAVE-small is a self-directed and workshop-based method in which a small team from within the organisation performs the risk assessment and analysis exercise. The OCTAVE-small method has four processes which involve identifying critical information assets, identifying threats to those critical assets, identifying current asset vulnerabilities, and performing risk evaluation and putting in place appropriate risk management strategy for that particular organisation. The use of the OCTAVE-small method provides the users of CISs with an opportunity to participate in all risk management exercises taking place in their organisations. This also empowers the users by encouraging them to be involved in decision making about the security posture of their organisations.

Threat profiles can be created using visual trees that show the critical asset, how it is accessed, who accesses it, the motive and the outcome. Four major categories of threats have been theoretically identified and the ways they could be used to build profiles are identified. However, in this study, simple customised tables were used instead of tree threat profiles. Data for this study were generated through observation, inspections and interviews of the participants, users of CISs. The next chapter, Chapter 7 focuses on empirical research in which data are generated, analysed, presented and interpreted.

CHAPTER 7

7. DATA ANALYSIS, PRESENTATION AND INTERPRETATION


PART I
INTRODUCTION AND RESEARCH METHODOLOGY
CHAPTER 1: INTRODUCTION
CHAPTER 2: RESEARCH METHODOLOGY
PART II
LITERATURE REVIEW
CHAPTER 3: INFORMATION SECURITY RISKS OVERVIEW
CHAPTER 4: RISK MANAGEMENT PROCESS
CHAPTER 5: RISK MANAGEMENT METHODOLOGIES
PART III
EMPIRICAL STUDY
CHAPTER 6: THE OCTAVE METHODOLOGY
CHAPTER 7: DATA PRESENTATION, ANALYSIS AND INTERPRETATION
PART IV
CONCLUSION
CHAPTER 8: RESEARCH CONTRIBUTION AND CONCLUSION

7.1. INTRODUCTION

The importance of information security risk management has been emphasised throughout the preliminary chapters of this study. A risk management exercise is essential to any security improvement initiative because it can generate an organisation-wide view of information security risks at the same time providing a baseline for improvement (Alberts *et al*. 2003). This implies that an effective information security risk management exercise considers both organisational and technological issues and examines how CISs users manage and use their organisation's computing infrastructure on a daily basis. This study is an initiative to afford secondary schools managers and CISs users an opportunity to perform risk management exercises for their CISs using the OCTAVE-small risk management method. Subsequently, secondary schools are expected to actively plan how to apply good security practices to address organisational and technical vulnerabilities that are likely to impact negatively on their information systems assets, hence improve service delivery.

The purpose of this chapter is to report on the empirical risk management case study undertaken in two selected secondary schools in Thohoyandou Cluster, Vhembe District.

The structure of this chapter includes background context of the two secondary schools involved in this study, an overview of data collection methods used for the case study. This is followed by identification of critical assets for CISs, threats, vulnerabilities and risk components in accordance with OCTAVE-small. Data is presented, analysed and interpreted qualitatively. Tentative findings are given thereof. Organisational vulnerabilities are treated first followed by technical vulnerabilities. A detailed description of the structured analysis of various threats, vulnerability and risk components is also given. Overall risk analysis is done and then followed by protection strategies and mitigation plans. A conclusion to the chapter is given at the end as a summary of what has been discussed in this chapter.

7.2. DESCRIPTION OF SCHOOLS INVOLVED (SCHOOLS A AND B)

Both Schools A and B (*names withheld*) are Government Further Learning and Training (FET) schools located in Thohoyandou Cluster, Vhembe District (Limpopo Province). The schools are in peri-urban suburban area and have high learner enrolments. The organograms of these schools are similar because they are prescribed by the Department of Education (DoE). Figure 7.1 shows the Organogram in general.

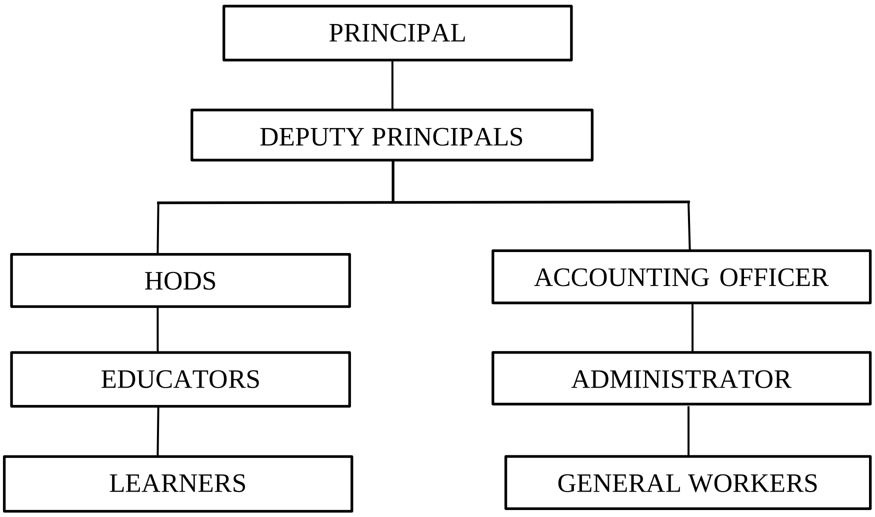


Figure 7.1: Schools A and B Organogram structure

Each secondary school had the following functional structures:

- a permanent administrative staff (all educators);
- permanent and temporary teaching staff;
- permanent general staff;
- learners from Grade 8 to 12; and
- a relatively large information technology infrastructure manned by administrative educators who were responsible for on-site computer and network maintenance and upgrades. The computers were located in different rooms and offices. Some computers were used for administrative purposes and others used for teaching purposes.

This research targeted those computers used for administrative purposes especially in the computerisation of information systems.

7.3. PREPARATORY ACTIVITIES

The success of the OCTAVE-small method depends on the financial and human resources support given to the collaborative team by the management (Alberts and Dorofee, 2003; Harper, 2002). In this research study school management provided support in the form of human resource and information systems assets. The compositions of the collaborative teams in the two secondary schools were similar. Table 7.1 is a summary of the collaborative team composition.

Table 7.1: Composition of the collaborative team

Team member	Area of specialisation	Information Technology skills	Duties performed
Administrative educators	Records management both computerised and manual	Basic hardware and application software skills	In charge of all computerised records and custodian of information technology assets. Installs and configures hardware and software in all office computers.
Accounting Officer	Accounting and basic computer skills	Fairly good user of computing facilities Very good in problem solving	Finance officer and custodian of all computerised and manual financial records.
Deputy principal	Education and management	Good operational skills in selected packages. Very good problem solver	Maintains a small database for staff records and hard copies of learner records. Uses Custom software to capture learners' marks.
Researcher	Information systems	Hardware and software expert	An outsider given the role to organise the collaborative team and facilitate meetings.

7.4. DATA COLLECTION

This study targeted all information assets that were used in CISs. These included:

- data or information collections such as databases, data files, policies, standards, procedures, information archives, disaster recovery/continuity plans or digital records;
- software assets such as application software for office automation, system software and custom software (locally developed programs);
- physical assets, such as computers (desktops, servers, laptops, portable digital assistance, tablets), communication equipment (modems, hubs), storage media

(removable disks, CDs/DVDS), and some facility equipment (generators, power supplies, air conditioners).

Data was generated through participatory observations, physical inspections and interview techniques discussed in Chapter 2 and 4. Alberts *et al*. (2003) argue that security concepts are embedded in OCTAVE-small worksheets and allowing the use of worksheets by less experienced personnel makes them (worksheets) more viable. These authors also encourage those who intend to use the OCTAVE-small method to customise the worksheets and implement them according to the organisation being studied. Therefore, complex and lengthy OCTAVE-small data collection worksheets were customised and integrated with the observation schedule, inspection checklist and interview schedule designed by the researcher. Customised OCTAVE-small worksheets were easy to use and relevant to the problem being studied.

7.5. OUTPUTS AND THE OCTAVE-SMALL METHOD

In this study, outputs define the results that collaborative teams achieved during the risk management exercise performed at each school. Alberts and Dorofee (2003) suggest that a particular output should be generated by a given activity in a definite OCTAVE-small process. Each output was then mapped onto the relevant OCTAVE-small process as shown in Table 7.2.

Table 7.2: Mapping of outputs to the OCTAVE-small method

Output	**Implementation in the OCTAVE-small method**
Critical assets for CISs	**Process 1**: Data was gathered through an asset identification and inspection checklist and interview of two key users of CISs in each school. This included members of the collaborative teams who eventually identified critical assets.
Organisational security practice to safeguard critical assets and areas of concern	**Process 1:** Data gathered through interviews of system users including collaborative team members
Security requirements for critical assets	**Process 2:** Users of CISs defined security requirements for their important assets. The collaborative team used this information to establish the security requirements for the school

Output	**Implementation in the OCTAVE-small method**
	critical assets.
Current security practices	**Process 2:** Users of information systems assets contributed their views on security practices currently being used by each school. Two users completed a simple security checklist. Follow-up discussions on key issues were made. Collaborative teams consolidated security practices
Threats to critical assets	**Process 2:** Collaborative teams inspected critical information systems assets to identify threats. Users of CISs were observed using assets and also interviewed on areas of concern. The collaborative teams used these areas of concern as input to create a threat profile for each critical asset in tabular form
Current organisational vulnerabilities	**Process 3:** Users of CISs contributed their views on missing or inadequate security practices in the schools (organisational vulnerabilities).
Key components	**Process 3:** Collaborative teams identified key components of the computing infrastructure. The teams used the critical assets and the threats to select key components.
Technical vulnerabilities	**Process 3:** Each collaborative team evaluated each key component using vulnerability evaluation tools like Windows Defender and antivirus. Manual checks for vulnerabilities on the network and computers were performed
Risks to critical assets	**Process 4:** Each collaborative team identified the potential impact of the threats to critical assets. A list of risks was produced in tabular form.
Protection strategy	**Process 4: C**ollaborative teams developed possible protection strategy for organisational security improvement. The strategy was based on organisational and technological vulnerability information.
Risk mitigation plans	**Process 4:** Collaborative teams developed risk mitigation plans to reduce the risks in CISs critical assets. Each team selected mitigation actions based on the organisational and technological information security risks identified throughout the evaluation process.

Source: Alberts and Dorofee (2003) with modification

The following sections describe what took place during each process based on activities which were carried out. The first process involved identifying critical assets in CISs in secondary schools.

7.6. PROCESS 1: IDENTIFY CRITICAL ASSETS IN COMPUTERISED INFORMATION SYSTEMS IN SECONDARY SCHOOLS

This process was carried out according to OCTAVE-small guidelines by Alberts *et al*. (2003). Data pertaining to information systems assets, current protection strategy practice and existing organisational vulnerabilities were gathered through interviews, observation, inspection checklists and OCTAVE-small customised worksheets. Information systems assets for each school were compiled, and then teams held discussions to compile lists of critical assets for each school.

7.6.1. Activity 1: Identify information system assets in secondary schools

The main purpose of this activity was to identify and locate all information systems assets used to support administrative activities. Observation checklists, interview schedules and inspection checklists were used to collect data from two key users of information systems in both schools. The interview also included security aspects of the information systems that the users experienced when they used identified assets. A sample of interview transcription is given in Appendix 4. An inspection checklist was also used to verify interview results. Two collaborative team members from each school completed an inspection checklist for their school. Data pertaining to information systems assets for each school were summarised and presented on Tables 7.3a and 7.3b below.

Table 7:3a: Asset identification and inspection checklist Secondary School A

	Important Asset	**Type**	**Location**
1.	Custom software applications	Application/software	Server – reception
2.	Learners CASS Mark and Schedules	Information	Server – reception
3.	Educators' information	Information	Vice Principals' offices
4.	Subject allocation lists	Information	Vice Principles' offices
5.	Asset management System	Application/Software	Server – reception
6.	Computers /Laptops	Hardware	Offices
7.	Modem	Hardware	Vice principal's office
8.	Switches/hubs	Hardware	Tea room
9.	Compact Disks	Hardware	Strongroom
10.	Financial information: Creditors payments and school fees information	Information	Strongroom Accountant's computer
11.	Network cables	Accessories	Administration block

Table 7:3b: Asset identification and inspection checklist Secondary School B

	Name of Asset	**Type**	**Location**
1.	Custom software application	Application/Software	Laptops in Strongroom and vice principal's computers and staffroom computers
2.	Learners' CASS Mark Schedules	Information	Office Computers & laptops in strong room
3.	Educators' personal information	Information	Vice Principals' computers
4.	Subject allocation lists	Information	Vice Principles' offices
5.	Asset management System	Application/Software	Vice Principals' computers
6.	Computers/ Laptops	Hardware	Offices
7.	Modem	Hardware	Office
8.	Compact Disks	Hardware	Strongroom
9.	Switches	Hardware	In the corridor of administration block
10.	Network cables	Accessories	Administration block
11.	Financial information	Information	Accounting Officer's Computer

Information on Table 7.3a and Table 7.3b shows that the two secondary schools had similar information systems assets used in their computerised information systems. School A had both wired and wireless LANS, which were in good state. School B had a wired

LAN only. The LANs were supported by broadband internet connections. All the assets indicated above were important for the operations of the schools. Each collaborative team proceeded to select critical assets for its school.

7.6.2. Activity 2: Selecting critical information systems assets

Discussions by collaborative teams led to the compilation of lists of critical assets for each school. The two lists were comparatively similar and were collapsed into a single list, Table 7.4. Reasons for selecting an asset as being critical are also given alongside.

Table 7.4: Critical assets in both secondary schools

Critical asset	Justification for its selection
Learners' CASS marks database	It stores CASS marks for all learners used for progress reports and final promotion at the end of the year. This information needs to be strictly secured from any changes, loss or viewing by unauthorised individuals. It also needs to be always available to school management.
Financial information: Creditors' records, school fees, salary records for general workers	This information is highly confidential and could only be accessed by the principals and Accounting Educator. SARS tax numbers, amount payable, service rendered or products delivered, payments information should be confidential and while retaining its authenticity. Its availability to the principals and auditors was also very important.
Custom application	It is used in data capturing and processing. Learners' computerised records are only accessed through this application. Its modification may result to unavailability of records management and disruptions.
Computers used in the administration offices	Most of the information is stored in these computers. The computers are used to access, retrieve, process and output the needed information.
Modems and hubs	Provide interconnection of all computers used in the school. Hubs provided connectivity and a means of accessing information on the server-computer and other computers with vital information. Modems were used for internet connections
Educators personal information	This information was supposed to be confidential and could only be accessed by the principals and administrative educators. Educator's persal number, SACE numbers, SARS tax numbers, sensitive reports on staff misconducts, monthly salaries.

Table 7.4 shows six information systems' critical assets for the two secondary schools involved in this study. Justification for selecting an asset as critical is also given. After identifying critical assets, the teams proceeded to evaluate organisational security practice taking into account the critical assets at hand.

7.6.3. Activity 3: Evaluate organisational security practices

A simple checklist was used to gather data on the state of information security from CISs users' point of view. This was intended to establish information security awareness among the users of CISs and the overall current security practices. One deputy principal and administrative educator from each school completed a checklist for their schools. Table 7.5 is a summary of results for security practices in both schools.

Table 7.5: Organisational security practices for Schools A and B

	Item	**Schools A and B**
1.	Information security policy	No written security policies
2.	Risk management	Neither of the school does risk management
3.	Access account management	No procedures to manage access accounts
4.	Configuration management	No control Plan
5.	Password authentication	No enforcement rules, optional, shared passwords
6.	Network security policy	No written internet or network policy.
7.	Modems policy	No policy in place.
8.	Cryptographic capability	No such capabilities existed.
9.	System administration	Administrative educator acts as a systems administrator mainly for software and hardware maintenance.
10.	Incident response capability	No policy for this. No training for users and systems administrator. Schools did not keep records for precious information security incidents.
11.	Viruses and malware policy	No policy. Use of virus protection mechanisms, but this is not mandatory. Some users could recognise virus effects, but other users were ignorant of viruses and their effects. Users were unable to clean malware
12.	Contingency planning	There is no contingency plan in place. Schools did not have UPSs to cater for unplanned power cuts.
13.	Backups policy	There is no backup policy but the backup is done periodically by any user who feels a need to.
14.	Maintenance policy	There is no policy. Maintenance was done by

	Item	Schools A and B
		Administrative educators when there were problems or schools employed outsiders to do maintenance.
15.	Media sanitisation	Rarely done. No policy for this. Only hard copies are burned or dumped at school dump sites.
16.	Physical security policy	No written physical security policies in both schools. However, all doors and windows to rooms with information assets are burglar barred. Modems and hubs are poorly secured can be removed easily. No zoning of the area where information systems are used.
17.	Personal security policy	There are no documented information security orientation courses for employees. No documents signed for non-disclosure of critical information.
18.	Training and awareness programmes	No documented programmes for training and awareness on information security. No training and awareness of information security were provided to information systems users

The results on organisational security practices on Table 7.5 indicate that both schools did not have written policies concerning information security. Besides physical security controls being enforced, the results indicate a deficiency in the security practice of the two schools that left critical information assets at risk from threats. Lack of training or awareness in information security was evident in both schools. It could be argued that information security was given little or no priority in both schools. Although schools appreciated the importance of CISs, there was clear evidence that their current organisational security practices disregarded this fact. This undermined the crucial role played by CISs assets in these schools.

Information systems users raised concerns pertaining to current security practice in the schools. The areas of concern are presented on Table 7.6.

Table 7.6: Areas of concern for critical information systems assets

Asset	Areas of Concern
Learner CASS	**Disclosure**

Asset	Areas of Concern
marks database	Some of the authorised users had a habit of accessing information they were not authorised to use. At times, legitimately accessed information was inappropriately distributed to wrong individuals like learners and community people who used it to attack school management during general meetings.
	Modification Authorised users intentionally entered erroneous marks to the advantage of some learners. Authorised users deliberately gave their friends access to confidential records, at times, they were influenced to modify the marks. The risk of an outsider's intrusion into the CASS database was more likely to occur because the inbuilt firewall systems on the server-computers were wrongly configured.
	Interruption/loss If the Administrative educators went on leave, some important functionality of the database and custom software could not be used. Custom software used on CASS database was incompatible with Windows 7 and crashed frequently disrupting capturing of marks. Power outages and other external events were likely to result in denial of access to CASS marks database. This essentially caused delays in the processing of termly schedules and reports.
	Loss/destruction Accidental or deliberate loss of any important information was a concern when unauthorised users deleted files while using the computers meant for administrative purposes.
Educators' information	**Disclosure** Authorised users unintentionally or intentionally disclosed confidential educator financial information to friends. There was no physical security in the reception where server-computers and sensitive information were kept. Unauthorised persons could wander in and see confidential information displayed on the workstations in these rooms.
	Loss/destruction, modification Authorised and unauthorised users could change or delete the information on educators upon opening files. Educators employed by schools end up receiving wrong salaries or not receiving any salaries at

Asset	Areas of Concern
	all. Incorrect information on insurance claims ends up being sent to SARS.
Financial records and service provider’s information	**Modification** Deliberate modification of the records resulted in schools getting poor services or substandard products from dubious providers. Some amounts on receipts were wrongly captured, understated or overstated and double payments made.
	Loss/destruction Invoices or receipts were being misplaced and could not be traced for verifications during auditing. This resulted in unpaid credits or double payments for the same product
	Disclosure Unauthorised users disclosed sensitive financial information they come across. Some information was printed and distributed unofficially to authorities
Computers	**Loss /destruction** Computers and hardware were easily moved by authorised and unauthorised persons. Hard disks could be replaced or damaged during these movements. Critical information would be lost. At times hubs went missing. Unauthorised users used memory sticks infected with viruses on administration computers thereby infecting them with different malware.
Custom software	**Modification** Custom software for accessing CASS database used a shared password which could easily be obtained from authorised users. Unauthorised users could use it to gain access to the database and modify learner’s marks.
	Disruption Schools complained of recurrent crashing of custom software on some computers. This caused unnecessary delays in processing of reports and results analyses.

Asset	Areas of Concern
	Loss/ Destruction Software installation folders could easily be deleted over the network. Software was prone to malware attack
Network	**Disruption** Network down-time was high due to hub problems

Information on Table 7.6 indicates that there were many concerns raised by CISs users that affected the security of the critical assets hence their use. The main concerns arose from unaccounted modification of critical information by some authorised users, divulging of critical information to unintended people and disruption of services due network problems.

The foregone activities identified critical assets and determined current security practices in both secondary schools. Security concerns pertaining to critical assets were raised by CISs users. The information obtained from these activities was then used in Process 2 which identified threats to critical assets.

7.7. PROCESS 2: IDENTIFY THREATS TO CRITICAL INFORMATION SYSTEMS ASSETS

In this process, collaborative teams identified security requirements for critical assets and threats to those critical assets. Data were gathered using customised OCTAVE-small worksheets. Some data were obtained from the interviews previously held in Process 1.

7.7.1. Activity 4: Identifying security requirements for critical assets

Discussions of security requirements led to the determination of the most important security requirements for each critical asset. The results for both schools were summarised and presented on Table 7.7 below.

Information on Table 7.7 indicates that the learners' CASS marks database should retain its integrity throughout. Only one authorised person, the administrative educator was supposed to alter those marks. This was confirmed by what the administrative educator in School A said about modification of CASS marks:

“In the event that one of the principals or data “capturer” makes changes to any of the marks using data capturing software or application on any other computer besides the server-computer, the program will report the changes and it is me who can confirm or reject the changes after verifying the mark affected. The only problem we have is that the system does not record somewhere the mark that would have been deleted. I have to look for the original marks schedule. These changes must be authorised by the deputy principal. If the changes are made on the server-computer, then it is difficult to detect this anomaly. The learner will benefit at the end”, (Administrative educator 1).

Table 7.7: Current security requirements for critical information systems asset

Critical asset	**Security requirements descriptions**	**Most important security requirement**	
Learners CASS marks database	Only one authorised person was supposed to modify CASS marks once they were saved. No unauthorised person should modify this information	Integrity	1
	Cass marks should be accessible at any time they are needed (at least 5 hours a day)	Availability	2
	Only authorised persons can view marks	Confidentiality	3
Financial records / information	Only the Accounting Officers should be authorised to modify this information with permission from the principals.	Integrity	1
	Only authorised persons should view these records.	Confidentiality	2
	Should be accessible all the time it is needed	Availability	3
Educators personal Information and Salaries	Alternations should be made by an authorised person.	Integrity	1
	Only authorised persons can view this information.	Confidentiality	2
	Should be accessible all the time the information is needed	Availability	3
Custom software	Should always be available and can be used by authorised persons	Availability	1
Computers	Should always function perfectly during school hours	Availability	1

Critical asset	Security requirements descriptions	Most important security requirement	
	Should be used by authorised personnel. No unauthorised person should use administrative computers	Integrity confidentiality	2 3
Routers and hubs	Should always be on during the day	Availability	1

Key: **1 = Most important security requirement,**
2 = Second most important security requirement
3 = Third important security requirement

In School B, the Administrative educator echoed the same sentiments in an interview: “We are always surprised that at the end some mark tampering would have occurred in some cases when we crosscheck for each learner”, (Administrative educator 2). It seems that schools find it difficult to maintain integrity of information stored in computers due to a number of known and unknown threats.

7.7.2. Activity 5: Identifying threats to critical assets

Collaborative teams examined threats and threat sources to each identified critical asset. Data were collected using customised OCTAVE-small threat profile worksheet. A number of mitigating factors led to customisation of OCTAVE-small worksheet:

- reducing the amount of paper work to be done and the time needed to gather data compared to when the conventional worksheets were used;
- some of the areas examined by the conventional OCTAVE-small did not apply to secondary school situations where there were no records of previous information security risk management exercises; and
- making the instrument user friendly to the collaborative team members.

This was in line with Alberts *et al.* (2003), Woody *et al.* (2006) and Panda (2009) who encourage organisations to customise OCTAVE-small worksheets to their needs. The results of this activity are shown on Table 7.8.

Table 7.8 below shows common threats/threat sources that were found in CISs critical assets in both schools. The effects of the identified threats on each critical asset and their overall impact on the schools are also documented on the above table. A number of threats/threat sources were related to human being actions, malware and environment in which the assets were used. The majority of the threats impacted negatively on school productivity, reputation and finance. The three information security requirements were also compromised. Information integrity and availability of critical assets were the most affected.

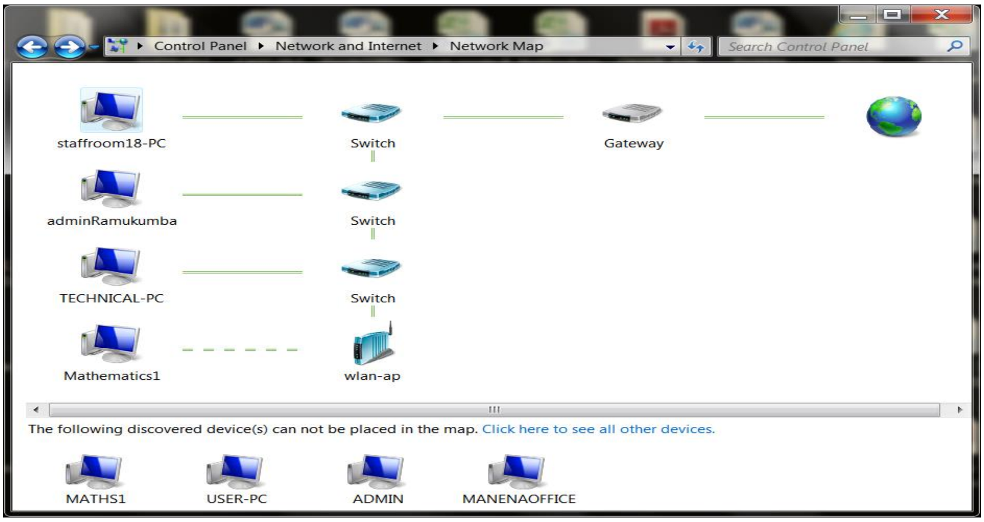
Table 7.8: Summary of threats/threat sources from asset risk profiles

Asset affected	**Threat/threat source**	**Possible threat effect or impact on asset**	**Potential impact on the school operations/ mission**
Learner CASS marks Database	Unauthorised users who accessed the server-computer over the network.	Deletion of database – *availability* affected Modification of records – integrity was compromised	Productivity was disrupted; financial loss through re-installation of software; distrust of school managers by learners and parents affected school reputation.
	Authorised users who accessed server-computer over network deliberately modified marks.	Information *integrity* compromised.	Some learners were promoted on the basis of falsified marks; school reputation was affected when learners with forged results were demoted.
	Unauthorised users gained physical access to server-computers and printed fake school reports.	Exposure impinging negatively on *confidentiality*. Information integrity at risk	Schools' reputation severely damaged when learners get results which mismatch their performances and fake results on school reports.
	Employees replacing, disconnecting or hiding hubs	Database *availability* to other computers is severely affected. Increases marks capturing time and leads to errors in data entry.	Disruption of operations that used the database. Productivity decreased. The schools lost money in replacing the hubs or paying workers overtime.
	Untimely and persistent system crashes	Destruction or corruption of files affected *availability* of systems.	Productivity was affected. Data were recaptured. Delays in meeting targets were experienced.
	Defective hard drive	Destruction of database, files irretrievable. *Availability* is severely affected	Productivity affected, loss of finance through buying new hard disks, hiring technicians to replace them.

Asset affected	**Threat/threat source**	**Possible threat effect or impact on asset**	**Potential impact on the school operations/ mission**
	Malware (Viruses and Trojan horse)	Infected database files and creating shortcuts. Corrupted records. Cleaning virus deleted the database files. *Availability* was affected	Data capturing and report printing were delayed. Reputation of schools was compromised.
Custom application software	Unauthorised users gain physical access and deliberately uninstall custom software	Mark capturing, processing and reports severely affected. *Availability* is compromised	Productivity and reputation were seriously affected. Termly marks capturing, mark schedules delayed. Schools have to pay the proprietor to reinstall system
	System crashes	Custom software sensitivity to system crashes corrupted it. Reinstallation was needed. *Unavailability* persisted for long time	Productivity is affected; report printing differed to a later date. Payments to be made to the proprietor for reinstallation
	Custom software incompatibility with Windows 7	System hanging when the Custom software was loaded. *Availability* was affected	Leads to loss of finance due to reconfiguring charges.
	Expired licences	System *availability* is affected. Records cannot be captured or processed.	No productivity in terms of CASS marks until the school pays for the licence renewal.
	Virus and Trojan horses	Prone to virus attacks. Some of its files are detected as malicious code by some antivirus. Affect *availability*. Users deleted some files as prompted by antivirus.	Schools pay for the malware removal, maintenance of the system. Schools always victims of bogus technicians who replace genuine components with pirated ones or sell fake antivirus.

Asset affected	**Threat/threat source**	**Possible threat effect or impact on asset**	**Potential impact on the school operations/ mission**
Financial Records (creditors payments and learners fees)	Unauthorised users used physical access to financial records when Accounting educator left workstations unattended.	The users could view and modify financial information for learners or creditors. Both *confidentiality* and *integrity* were affected	Loss of revenue due to double payment or uncollected fees. Unpaid creditors may disrupt services in the school. Some users discuss about the amounts paid to some creditors, this discredits the school.
	Virus and Trojan horses	Data corruption compromises *integrity*. Accounting software failed to load, needed reinstallation; availability was affected.	All school operations that depend on this information asset are either suspended or slowed down. School reputation with creditors was likely to be negatively affected.
Computers	Unauthorised removal of hardware	Disrupts network and makes it *unavailable*	Productivity was affected negatively
	Theft of computer components by authorised and unauthorised users	Permanent loss of data and computers unusable. *Availability* was compromised	Productivity and financial loss by schools
	Poorly air-conditioned rooms resulting to high temperatures	Computers overheating and crashing. Systems become unavailable	Productivity and reputation of schools at stake
	Power outages	Destroys hardware. Computers become unusable. *Availability* was compromised	Loss of data and money as computer needs to be replaced
Network bandwidth	Illegal connection of laptops and other portable devices to the school network	Accessibility of server-computer by applications on workstations serious impaired. *Availability* compromised.	Productivity for that particular day seriously negatively affected.

In both schools CASS marks databases were on server-computers and were shared so that three other computers (Administrative educators and two Vice Principals) accessed databases over the school LANs. Custom application software, another critical asset, was being used to access the database. In School A, the LAN consisted of more than twelve computers while at School B, there were 10 computers. There were two major weaknesses with these two critical assets; all users shared one password which each school was unable to change; and shared folders on the server-computer were visible over the LAN. Figure 7.2 shows the LAN architecture for School A obtained after running the network device discovery program from a LAN workstation in one of the staffrooms being used by educators for various purposes.



The following discovered device(s) can not be placed in the map. Click here to see all other devices.

Figure 7.2: LAN architecture for School A from staffroom

Figure 7.3 shows fourteen computers and media devices on School A LAN.

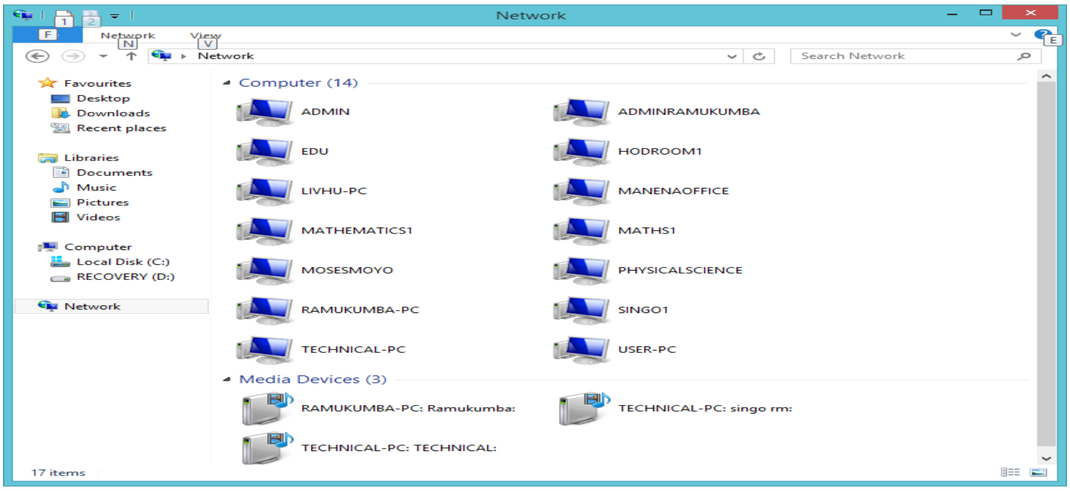
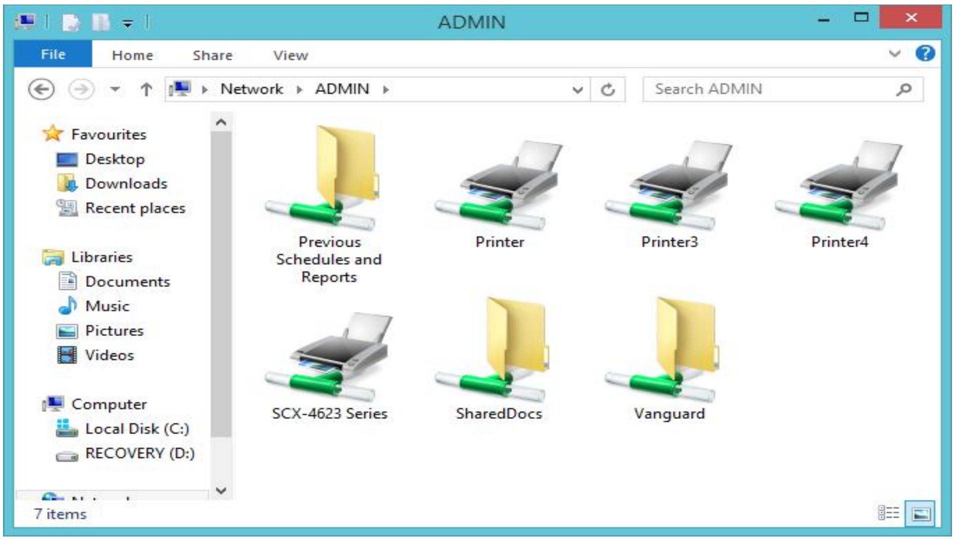


Figure 7.3: Computers on LAN in School A

Computers of interest were:

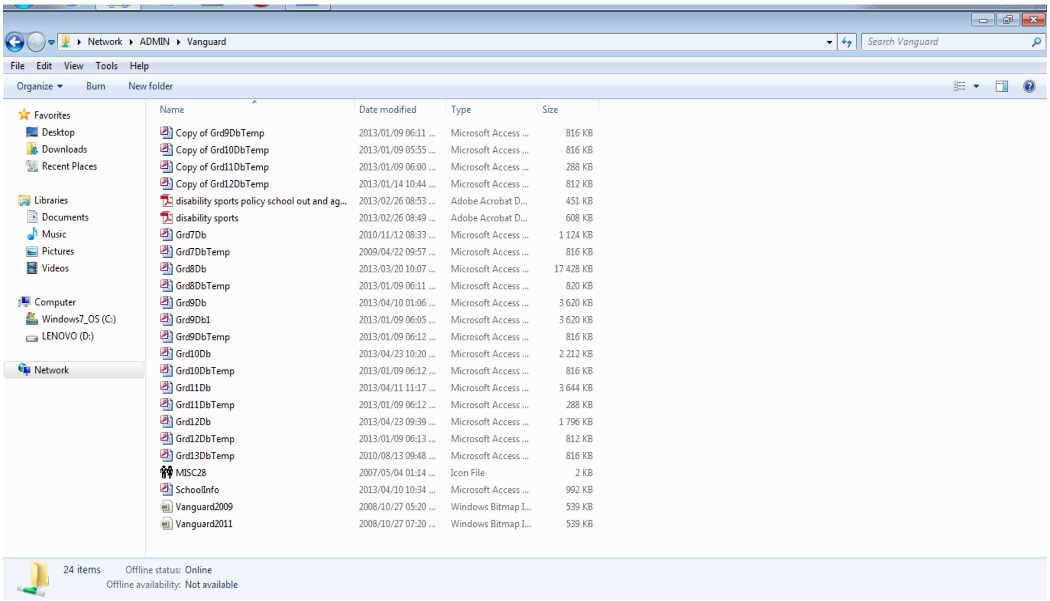
- ADMIN – the server-computer in which the CASS marks database was stored;
- adminRamukumba – a workstation storing financial information for the school. This computer was used solely by the accounting officer
- TECHNICAL-PC – a workstation in the vice principal's office that contained educator's information, mark schedules and installed with custom software to access the database on server-computer.
- MANENAOFFICE – a workstation in another vice principals office. This computer stored sensitive educators' information. It was also installed with the custom software to access the database.
- USER-PC – a workstation used by the Administrative educator to access the server-computer. The computer stores many types of documents used for the operation of the school.
- LIVHU – PC, USER-PC and EDU are computers illegally connected to school LAN

When ADMIN computer was accessed using a computer in a staffroom important folders were displayed as shown on Figure 7.4 below.



<u>Figure 7.4: Shared folders on the ADMIN Computer</u>

Important learners' CASS information is stored in *Previous Schedules and Reports* and Vanguard folders. The contents of these folders are also accessible as shown in figure 7.5 below.



Name	Date modified	Type	Size
Copy of Grd9DbTemp	2013/01/09 06:11 ...	Microsoft Access ...	816 KB
Copy of Grd10DbTemp	2013/01/09 05:55 ...	Microsoft Access ...	816 KB
Copy of Grd11DbTemp	2013/01/09 06:00 ...	Microsoft Access ...	288 KB
Copy of Grd12DbTemp	2013/01/14 10:44 ...	Microsoft Access ...	812 KB
disability sports policy school out and ag...	2013/02/26 08:53 ...	Adobe Acrobat D...	451 KB
disability sports	2013/02/26 08:49 ...	Adobe Acrobat D...	608 KB
Grd7Db	2010/11/12 08:33 ...	Microsoft Access ...	1 124 KB
Grd7DbTemp	2009/04/22 09:57 ...	Microsoft Access ...	816 KB
Grd8Db	2013/03/20 10:07 ...	Microsoft Access ...	17 428 KB
Grd8DbTemp	2013/01/09 06:11 ...	Microsoft Access ...	820 KB
Grd9Db	2013/04/10 01:06 ...	Microsoft Access ...	3 620 KB
Grd9Db1	2013/01/09 06:05 ...	Microsoft Access ...	3 620 KB
Grd9DbTemp	2013/01/09 06:12 ...	Microsoft Access ...	816 KB
Grd10Db	2013/04/23 10:20 ...	Microsoft Access ...	2 212 KB
Grd10DbTemp	2013/01/09 06:12 ...	Microsoft Access ...	816 KB
Grd11Db	2013/04/11 11:17 ...	Microsoft Access ...	3 644 KB
Grd11DbTemp	2013/01/09 06:12 ...	Microsoft Access ...	288 KB
Grd12Db	2013/04/23 09:39 ...	Microsoft Access ...	1 796 KB
Grd12DbTemp	2013/01/09 06:13 ...	Microsoft Access ...	812 KB
Grd13DbTemp	2010/08/13 09:48 ...	Microsoft Access ...	816 KB
MISC28	2007/05/04 01:14 ...	Icon File	2 KB
SchoolInfo	2013/04/10 10:34 ...	Microsoft Access ...	992 KB
Vanguard2009	2008/10/27 05:20 ...	Windows Bitmap I...	539 KB
Vanguard2011	2008/10/27 07:20 ...	Windows Bitmap I...	539 KB

24 items Offline status: Online
Offline availability: Not available

Figure 7.5: Files in School A database

Some of these files could be opened and data modified or deleted over the LAN. There was a high possibility that unauthorised and authorised users accessed the CASS database over the network and modified marks without being detected. This could lead to loss of integrity, confidentiality and availability.

Besides the learners' CASS database, all other critical information assets were accessible physically. Further observations and interviews revealed that there were serious concerns pertaining to threats and threat sources in critical assets. Table 7.9 shows areas of concern that were raised by users and management.

Table 7.9: Areas of concern pertaining to threats in critical assets

	Area of concern arising from	Affected information systems asset	Cited examples	Effects on critical information system asset
1.	Insiders using network access	Learners' CASS database Educators' profile information	Authorised users modified learner marks illegitimately Discussion of learners or educators with outsiders	Integrity and confidentiality were compromised
2.	Outsiders using network access	Learners' CASS database	Unauthorised modification of records or deleting important files	Integrity and availability were always compromised

	Area of concern arising from	**Affected information systems asset**	**Cited examples**	**Effects on critical information system asset**
3.	Insider using physical access	Learners' CASS Database Financial records Network hubs Backup disks	Tempering with marks of learners. Copying, printing, deleting or altering records Deleting it or changing subject allocation Hubs were off or data cables were disconnected Misplaced or scratched to make them unreadable	Renders marks unreliable Confidentiality, availability and integrity were compromised. Asset no longer available and creates chaos at school Disrupts network, networked resources no longer available. Backup files no longer available.
4.	Physical configuration problems	Information Hubs Data cables	Information on screen always visible to unauthorised users. Hanging where they can easily be removed or stolen Dangled outside where passers-by could destroy them	Loses confidentiality Loss of networked resource availability Loss of networked resources
5.	Software defects	Custom software	Hides some of the important forms Miscalculates values	Availability of the system is impaired. Unreliable results were produced.
6.	System crashes	Custom Software Operating systems	Occasionally hangs when entering data Crashes when running custom software	Availability is impaired and data is lost.
7.	Hardware defects	Hard disks Memory sticks External hard	Irrecoverable data loss occurred. Whole system disappears.	Availability seriously compromised

	Area of concern arising from	**Affected information systems asset**	**Cited examples**	**Effects on critical information system asset**
		disks	Required formatting resulting in loss of valuable information	Loss of important data
8.	Malicious code	Financial Information in files	Creates shortcuts for existing folders and data files. The original files disappear and cannot be opened. File corruption occurs	Information availability is lost. Data integrity is threatened
9.	Other problems	Information	Users forgetting names of files containing crucial information	Availability is affected

Identification of threat to information systems assets was completed successfully and results were presented in various tables then analysed and interpreted accordingly. Attention was then focussed on Process 3, infrastructure vulnerabilities identification.

7.8. PROCESS 3: IDENTIFY INFRASTRUCTURE VULNERABILITY

The goal of vulnerability identification is to determine the weaknesses or flaws in a system (Walsh, 2011). The activities performed in this section targeted technical vulnerabilities, vulnerabilities associated with computer hardware or software used in CISs. Technical vulnerabilities are weaknesses found in the technological infrastructure that could lead directly to unauthorised actions (Woody *et al*. 2006). To accurately identify vulnerabilities, Walsh (2011) encourages the team to first assess existing security controls in the systems of interest. In this research study collaborative teams resolved that if a control was missing then it was obvious that there was vulnerability in that component. The first activity was identification of key components of systems of interest, then examining access paths to critical information assets. This led to analysis of technology related processes.

7.8.1. Activity 6: Examining access paths

The examination of access paths involved identifying the key components of systems of interest that were closely related to critical information systems assets. Collaborative teams identified Learner CASS mark databases, financial records and computers as the most important critical assets for each school. It was concluded that the CASS marks database was most likely to be attacked from external and internal because it was on the LAN, while financial records were likely to be attacked from internal only. Certain information systems assets were likely to be used in these attacks. Such assets were referred to as key components. The key components included the server-computer, routers, hubs, data cables, the office workstations, educator's laptops and learners' mobile devices. It was established that most of the personal computers and laptops connected to School A LAN were able to access CASS marks databases on the server-computer. Access paths to critical assets were provided by class components which were studied.

Table 7.10: Systems of interest and key classes of components

<table>
<tr><th colspan="2">RECORDS MANAGEMENT SYSTEM</th></tr>
<tr><td><b>System(s) of interest</b></td><td>Learners' CASS marks database</td></tr>
<tr><td><b>Key classes of components used to access this critical asset</b></td><td>Server-computer
Desktop workstations
Laptops
Router
Hubs
Networking components (Both Ethernet and Wireless LANs)
Storage devices</td></tr>
<tr><th colspan="2">COMPUTERISED SCHOOL FINANCIAL RECORDS</th></tr>
<tr><td><b>System(s) of interest</b></td><td><b>Financial information</b></td></tr>
<tr><td><b>Key classes of components used to access this critical asset</b></td><td>Desktop workstations
Laptops
Router
Hubs
Storage devices</td></tr>
<tr><th colspan="2">Personal Computers (workstations and laptops)</th></tr>
<tr><td><b>System(s) of Interest</b></td><td>Personal computers were themselves the system of interest (they were) also a subsystem of the other systems such as Learner CASS marks database and financial information.</td></tr>
<tr><td><b>Key classes of components used to access this critical asset</b></td><td>Desktop workstations share same network components as the information assets above</td></tr>
</table>

Table 7.10 shows the system of interest and the key classes of components for each of the critical assets which the collaborative teams identified for evaluation. Reasons for selecting each system of interest and its class components are also given on the above table.

Table 7.11 shows systems of interest that were closely associated with critical information systems assets for the two secondary schools studied. On-site workstations, laptops and cell phones could possibly be used to launch attacks on data mainly through the internal networks. Information and data files stored on server-computer's hard drives were mostly prone to attacks through the internal network access points. Information and data on some workstations could be attacked through physical access methods that required the attacker to physically get hold of the system on which data were stored. Network devices like hubs and routers could either be disabled or removed to disrupt the network services thereby negatively affecting the availability of the critical assets such as CASS marks databases.

Table 7.11: Key classes of components and reasons for their selections

Class of Component	Reason for selection
Server-computer	CASS database stored and processed on the server-computer.
Networking components	Router / hubs provide connectivity and main access to LAN and internal/external access.
Security components	Firewall – key part of security for external access to office computers.
Desktop workstations	Used for all internal access to server and other desktop computers. Financial records are stored on a desktop workstation
Laptops	Used for internal and external access to the server computer
Storage devices	Provide storage media for the critical information
Wireless components	Provide connectivity and illegal access to school LAN

After establishing systems access paths, physical security checks on each critical information systems assets were performed taking into account the environment in which the assets were located and used. An observation checklist was used and the results are displayed on Table 7.12 below.

Table 7.12: Observation results for physical security threats

Asset	Location	Threats identified
Learners CASS marks Databases	Server-computer	Authorised users showing unauthorised users how to access the databases over the network Unauthorised users having access and tampering with files and information on the database or even deleting database files
Financial information	Financial Admin Computer	Authorised users accessing records they are not authorised to view or modify Unauthorised users who have motives to modify or delete records
Personal computers	Offices	Curious authorised users opened files with sensitive information and even modified or deleted files. Unauthorised users gain access through dubious means and tamper with data stored in the databases. Overheating results from poor air-conditioning damaged data storage systems Users' indiscriminate formatting of hard disks led to loss of vital data and information. Power supplies damaged by power surges Power cuts resulting to complete or partial data loss
Network hubs	Tea room	Tea room users unplugging the hub from power supply or even removing them from hangers, unplugging data cables. At times school hubs were replaced with malfunctioning hub from outside Unauthorised users plugging their laptops on extra ports to gain access to the School LANS
Routers	Office	Authorised and unauthorised users gain access to MAC address used to enter the wireless network.
Software disks	Strongroom	Authorised users misplacing backup or installation disks resulting in loss of valuable software, data and information Unauthorised users get software disks from authorised users and make pirated copies for their personal gains
Backup disks	Strongroom	Authorised users forgetting to label disks with backup data. Disks end up in hands of unauthorised users. Data files not password protected or encrypted

Information on Table 7.12 shows that threats to critical assets did exist. The observations made were consistent with previous data on the main threats to the critical assets.

It was also observed that the Ethernet LAN spent most of the time down due to the problems of the hub. Checks on the hub indicated that it was frequently unplugged by staff members who used the same power socket for cooking purposes. Figure 7.6a shows the hub in the tea room in School A.

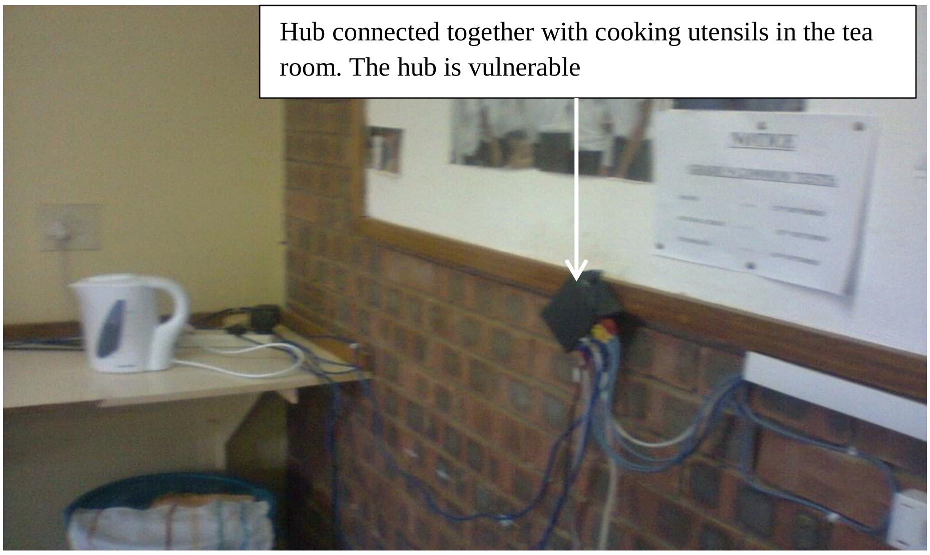

Hub connected together with cooking utensils in the tea room. The hub is vulnerable

Figure 7.6a: Switch connected together with water mugs in the tea room

Unsecured hub could easily be stolen / replaced with another or damaged if dropped on the hard floor. Another threat arose from the dangling data cables that could easily be snapped into pieces or dragged on the ground during sweeping, shown in Figure 7.6b

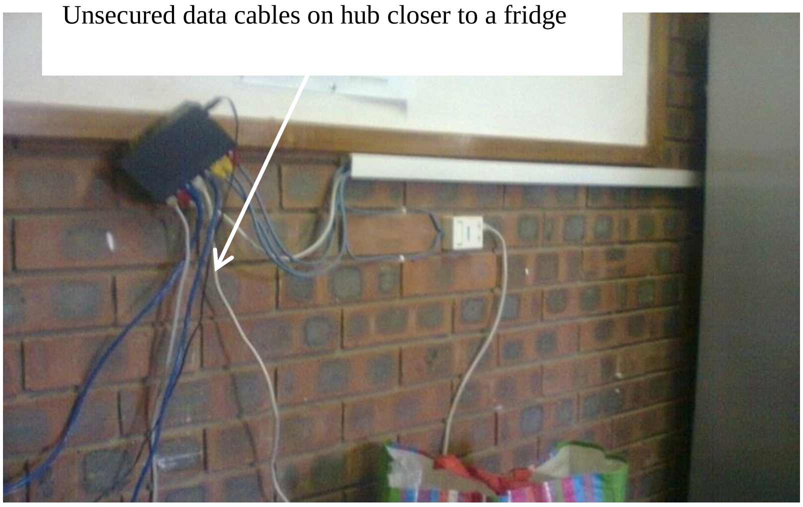


Figure 7.6b: Network hub closer to a refrigerator in tea room

Figure 7.7 shows a router in the vice Principals' office in School A. It was observed that the occupant of this office spent most of the time outside the office while the office door was unlocked. Unauthorised users utilised this chance to obtain the Media Access Control (MAC) address from the router and used it to plug their laptops or mobile devices to the wireless network.

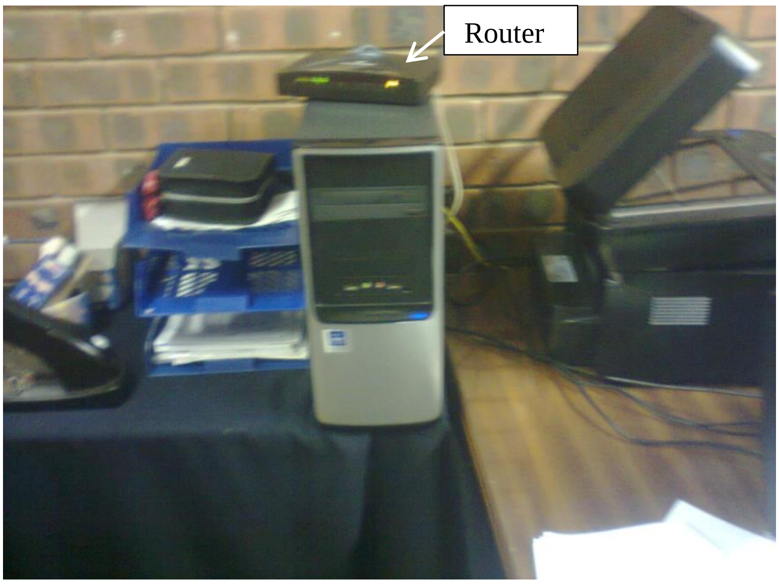


Figure 7.7: Unsecured router in unsecured office

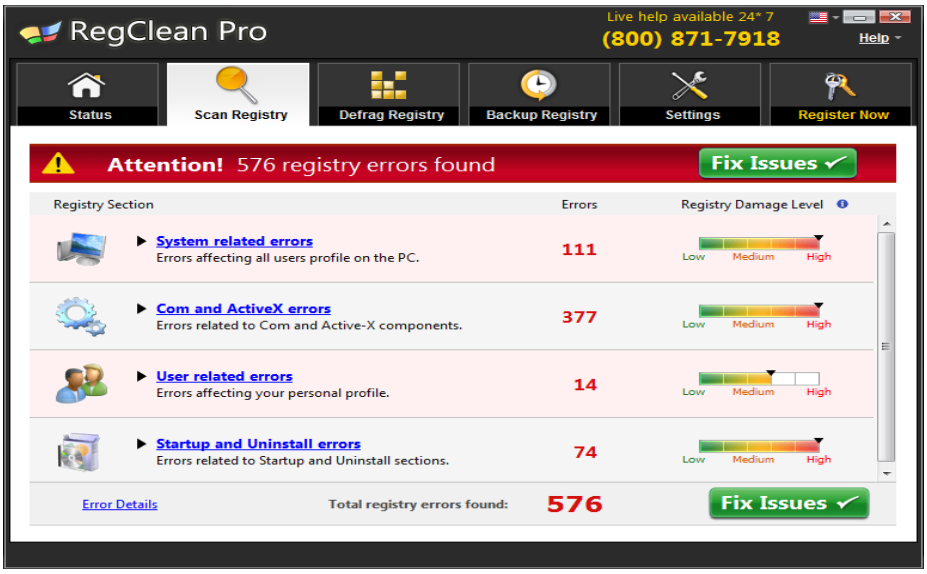
Simple system vulnerability checks were performed on hardware and software. The vulnerability checks were done while information systems assets were in use. An observation checklist was used to collect data during the systems vulnerability checks. Table 7.13 shows results for system vulnerability checks on the server-computers and other key components to the critical information assets.

Table 7.13: Observed vulnerabilities in the information systems

Target area	Observed Vulnerabilities	Comments
Access to computers and servers	No passwords on computers storing critical information	Easy access to data files likely to lead to deletion or modification of information
Access to custom software	Authorised users used a single password	Misuse of password by authorised users led to malicious attack by unauthorised users
Databases visible over the LAN	The database was visible to all computers on the LAN.	Deletion or copying of files over the network.
Access to	Easy to open tables and	Deletion of files by unauthorised user

Target area	Observed Vulnerabilities	Comments
databases	reports over the network	
Access to data in tables	Data can be inserted, or edited directly over the network.	Data modification.
Firewall settings	Firewalls disabled or wrongly configured.	Intruders or authorised users capitalise on this to gain access to sensitive information using portable devices
Antivirus installations	Installed but out-dated or expired licences. Some computers not installed with antivirus	Could not detect new viruses Easily infected and become sources of viruses
Illegal downloaded and installed shareware like games	Shareware downloaded from the Internet allowed users to play games on computers holding critical information.	Create security weakness that malware can utilise
Malware	Most detected malware could not be cleaned easily.	Infected computer were either very slow, information was also corrupted.
Network bandwidth	Excessive use YouTube to view music videos by authorised users	Wastage of data bundles leading to school paying high Internet costs
System restore points	Disabled	Cannot restore computer in case of crashes
System maintenance	Rarely done, no registers of vulnerabilities kept	Same attacks recurred frequently but no written records were made
Security of wireless LAN.	Less secured MAC address easily accessible.	Illegal connections of laptops and portable devices such as cell phones on LAN
Security of Ethernet LAN	No security password needed	Unauthorised connections successful from offices
Windows defender	Turned off, disabled /out-dated	No vulnerability scans done
Web-based e-mails	Frequently used on all administration computers	Users download attachments which at times contained viral infections
Internet connection	All computers access internet	Extensive use of the web and downloading of materials from dubious sites not monitored

Simple security vulnerability and virus scans were performed on server-computers using RegClean Pro, Windows Defender and antiviruses. The results of the vulnerability scanning using RegClean Pro and AVG PC analyser are shown on Figures 7.8a and 7.8b below. Results for malware scans are displayed on Table 7.14.



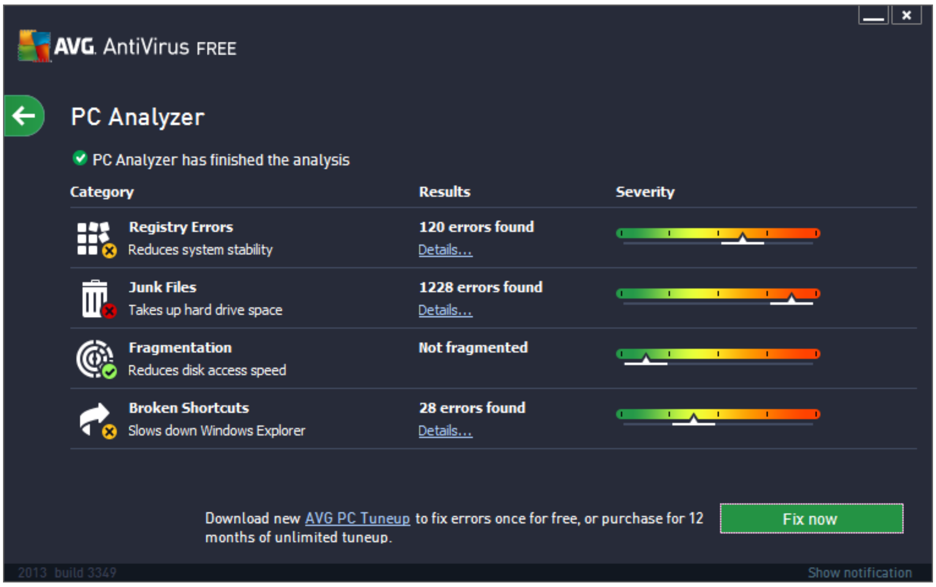
Attention! 576 registry errors found

Registry Section	Errors	Registry Damage Level
System related errors Errors affecting all users profile on the PC.	111	Low Medium High
Com and ActiveX errors Errors related to Com and Active-X components.	377	Low Medium High
User related errors Errors affecting your personal profile.	14	Low Medium High
Startup and Uninstall errors Errors related to Startup and Uninstall sections.	74	Low Medium High

Error Details   Total registry errors found: **576**   Fix Issues ✓

Figure 7.8a: Vulnerability scan results for School A Server-computer

The scan result showed 576 registry-related errors on the server-computer making it highly vulnerable to attacks. Correction of these errors resulted in the server-computer crashing after restart.



PC Analyzer

✓ PC Analyzer has finished the analysis

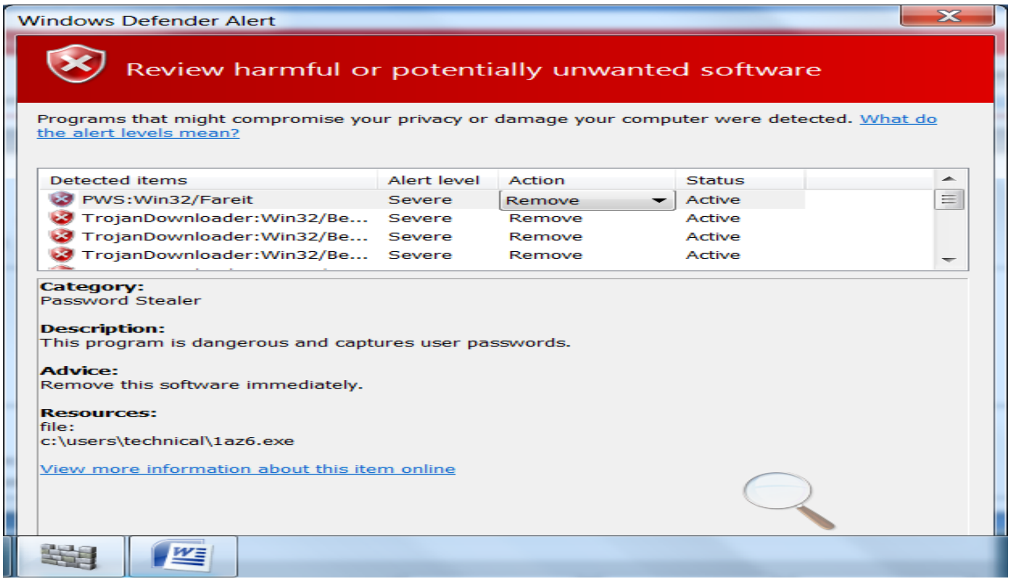
Category	Results	Severity
Registry Errors Reduces system stability	**120 errors found** Details...	
Junk Files Takes up hard drive space	**1228 errors found** Details...	
Fragmentation Reduces disk access speed	**Not fragmented**	
Broken Shortcuts Slows down Windows Explorer	**28 errors found** Details...	

Download new AVG PC Tuneup to fix errors once for free, or purchase for 12 months of unlimited tuneup.

Figure 7.8b: Vulnerability scan for School B Server-computer

The following figures also show results of basic vulnerability scanning done on server-computers in both schools. Windows defender and installed antiviruses (AVG and Norton) were used. In School A, the Windows Defender on the Server-computer was turned off.

Users were ignorant of the existence of Windows Defender. A number of malware was detected when Windows defender was used to scan the computers. Scan results are on Figure 7.9a and the result of cleaning the malware are shown on 7.9b, 7.10 and 7.11.



Windows Defender Alert

Review harmful or potentially unwanted software

Programs that might compromise your privacy or damage your computer were detected. What do the alert levels mean?

Detected items	Alert level	Action	Status
PWS:Win32/Fareit	Severe	Remove	Active
TrojanDownloader:Win32/Be...	Severe	Remove	Active
TrojanDownloader:Win32/Be...	Severe	Remove	Active
TrojanDownloader:Win32/Be...	Severe	Remove	Active

Category:
Password Stealer

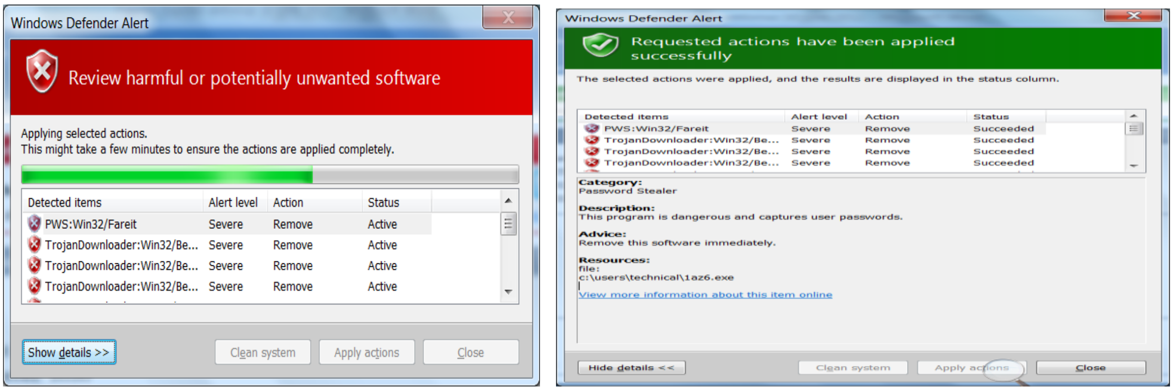
Description:
This program is dangerous and captures user passwords.

Advice:
Remove this software immediately.

Resources:
file:
c:\users\technical\1az6.exe

View more information about this item online

Figure 7.9a: Malware scan on School A server-computer



Windows Defender Alert

Review harmful or potentially unwanted software

Applying selected actions.
This might take a few minutes to ensure the actions are applied completely.

Detected items	Alert level	Action	Status
PWS:Win32/Fareit	Severe	Remove	Active
TrojanDownloader:Win32/Be...	Severe	Remove	Active
TrojanDownloader:Win32/Be...	Severe	Remove	Active
TrojanDownloader:Win32/Be...	Severe	Remove	Active

Windows Defender Alert

Requested actions have been applied successfully

The selected actions were applied, and the results are displayed in the status column.

Detected items	Alert level	Action	Status
PWS:Win32/Fareit	Severe	Remove	Succeeded
TrojanDownloader:Win32/Be...	Severe	Remove	Succeeded
TrojanDownloader:Win32/Be...	Severe	Remove	Succeeded
TrojanDownloader:Win32/Be...	Severe	Remove	Succeeded

Category:
Password Stealer

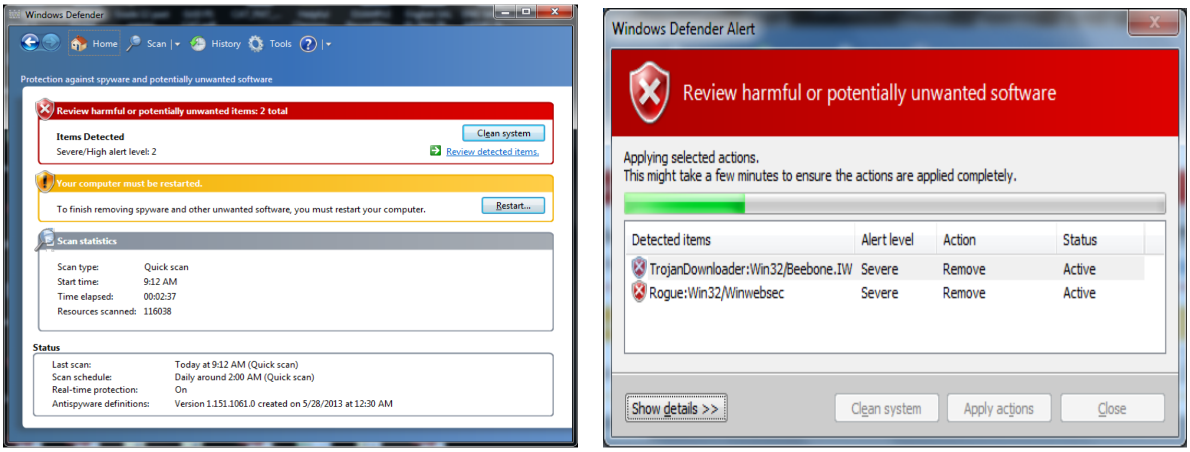
Description:
This program is dangerous and captures user passwords.

Advice:
Remove this software immediately.

Resources:
file:
c:\users\technical\1az6.exe

View more information about this item online

Figure 7.9b: Cleaning process and final results server-computer School A



Windows Defender

Protection against spyware and potentially unwanted software

Review harmful or potentially unwanted items: 2 total

Items Detected
Severe/High alert level: 2

Your computer must be restarted.

To finish removing spyware and other unwanted software, you must restart your computer.

Scan statistics

Scan type: Quick scan
Start time: 9:12 AM
Time elapsed: 00:02:37
Resources scanned: 116038

Status

Last scan: Today at 9:12 AM (Quick scan)
Scan schedule: Daily around 2:00 AM (Quick scan)
Real-time protection: On
Antispyware definitions: Version 1.151.1061.0 created on 5/28/2013 at 12:30 AM

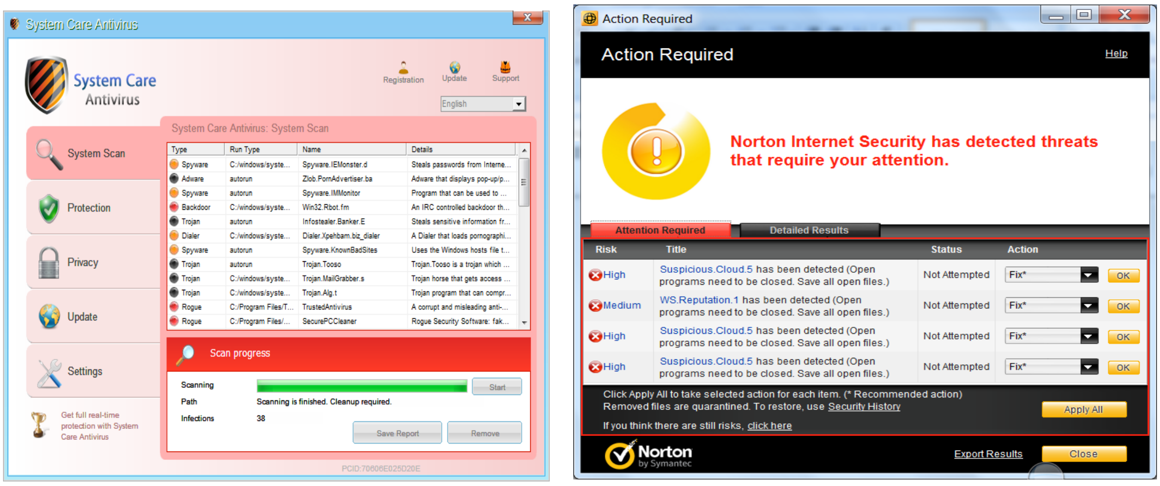
Windows Defender Alert

Review harmful or potentially unwanted software

Applying selected actions.
This might take a few minutes to ensure the actions are applied completely.

Detected items	Alert level	Action	Status
TrojanDownloader:Win32/Beebone.IW	Severe	Remove	Active
Rogue:Win32/Winwebsec	Severe	Remove	Active

Figure 7.10: Malware scanning and cleaning for School B Computer



System Care Antivirus: System Scan

Type	Run Type	Name	Details
Spyware	C:/windows/syste...	Spyware.IEMonster.d	Steals passwords from Interne...
Adware	autorun	Zlob.PornAdvertiser.ba	Adware that displays pop-up/p...
Spyware	autorun	Spyware.IMMonitor	Program that can be used to ...
Backdoor	C:/windows/syste...	Win32.Rbot.fm	An IRC controlled backdoor th...
Trojan	autorun	Infostealer.Banker.E	Steals sensitive information fr...
Dialer	C:/windows/syste...	Dialer.Xpehbam.biz_dialer	A Dialer that loads pornographi...
Spyware	autorun	Spyware.KnownBadSites	Uses the Windows hosts file t...
Trojan	autorun	Trojan.Tooso	Trojan.Tooso is a trojan which ...
Trojan	C:/windows/syste...	Trojan.MailGrabber.s	Trojan horse that gets access ...
Trojan	C:/windows/syste...	Trojan.Alg.t	Trojan program that can compr...
Rogue	C:/Program Files/T...	TrustedAntivirus	A corrupt and misleading anti-...
Rogue	C:/Program Files/...	SecurePCCleaner	Rogue Security Software: fak...

Scan progress

Scanning

Path: Scanning is finished. Cleanup required.

Infections: 38

Get full real-time protection with System Care Antivirus

PCID:70606E025D20E

Norton Internet Security has detected threats that require your attention.

Risk	Title	Status	Action
High	Suspicious.Cloud.5 has been detected (Open programs need to be closed. Save all open files.)	Not Attempted	Fix*
Medium	WS.Reputation.1 has been detected (Open programs need to be closed. Save all open files.)	Not Attempted	Fix*
High	Suspicious.Cloud.5 has been detected (Open programs need to be closed. Save all open files.)	Not Attempted	Fix*
High	Suspicious.Cloud.5 has been detected (Open programs need to be closed. Save all open files.)	Not Attempted	Fix*

Click Apply All to take selected action for each item. (* Recommended action)
Removed files are quarantined. To restore, use Security History

If you think there are still risks, click here

Figure 7.11: Virus scanning results – Administrative educators’ computer School A

The information on malware displayed on the above figures is a clear indication that critical assets such as data/information and application software were under threat. Table 7.14 is a summary of the most common malware found in computers in Schools A and B.

Table 7.14: Summary of malware scanning

School	Class of Component	Tool/ Method	Results	Vulnerability Summary
A	Server-computer	Windows Defender	- *trojandownloader.win32 /adload.da*	Severe: injects harmful code to Windows’ svchost.exe file
			- *PWS:Win32/Fareit:*	Severe: Password stealer
			- *Win32/TrojanDownloader.Bredolab.AA*	Server: downloads and execute files
			- *rogue:Win32/Winwebsec (System Care antivirus)*	Severe: Phishing software. Stops other programs to be executed
		Norton antivirus	- *Suspicious.Cloud 5*	Severe: makes a computer vulnerable to remote attacks that lead to identity theft; can block malware removal tools and system utilities such as Task Manager
B	Server-computer	Windows Defender	- *trojanDownLoader:Win32/Beebone.IW*	Severe: Downloads and installs other software silently
			- *rogue:Win32/Winwebsec*	Severe: Phishing software. Stops other programs to be executed
		Antivirus	*Expired*	No protection

Source: Microsoft help and support (2013)

Computers infected were observed to be slow in booting, loading applications and processing records. Technical information on detected malware indicated that:

- ***Trojan Downloader: Win32/Adload.DA*** silently downloads other programs from remote locations, sends users links that point to a Trojan code or malicious web address (Pilici, 2013). Its execution causes injection of harmful code to *Windows' svchost.exe file* (Pilici, 2013). The Trojan also infects wmicucit.exe by injecting its code to the last section of it. It is polymorphic in nature and endangers other executable files located on removable USB drives and network shared drives.
- ***PWS:Win32/Fareit*** is used to steal sensitive account information such as server names, port numbers, login IDs and passwords from clients' files, cloud storage programs or a host of installed files from the affected computer and sends it to a remote attacker in which a Distributed Denial of Service (DDoS) component. *DDoS: Win32/Fareit.gen!A*, is then commanded to perform flooding attacks against servers or computers holding sensitive information.

Basic vulnerability scanning provided the teams with insights into the inherent threats to CISs. Most of the vulnerabilities were severe as they caused loss of data and disruptions that led to reduced productivity and negative impact on school reputation. The teams progressed to the next activity of analysing technology-related process.

7.8.2. Activity 7: Analyse technology-related processes

This activity focused on the problems that were related to technology and their effects on the CISs. Data was gathered using an observation checklist. The results obtained are shown on Table 7.15 below.

The results on Table 7.15 above indicate that CISs in both secondary schools were vulnerable to threat attack. Many serious deficiencies in the software or hardware contributed to these vulnerabilities. Most of the problems related to technology were frequently experienced and had negative impact on the school operations that relied on CISs. Secondary schools had no controls in place to prevent attacks through these vulnerabilities.

Table 7.15: Frequently encountered hardware and software problems

Problem	**Effects**	**Control in place**
Hard disk failures	Loss of data, disruptions	None
System crashes	Loss of data and productivity time	None
Power failure	Hardware damages, data loss and disruptions	None
Network down time	Disruptions due to loss of availability	None
Malware	Data loss, system crashes, hiding files, disruptions	Antivirus
Wrong system configurations	System crashes leads to disruptions and data loss	None
Operating system related	System crashes leads to disruptions and data loss	None
Software conflicts	System crashes, loss of service, disruptions	None
Corrupted files	Loss of data and/or system crashes, disruptions	Backup
System hanging	Loss of service leads to disruptions	None
Damaged backup disks	Loss of data, productivity affected	None
Missing hardware	System unusable, loss of service, disruptions	None
Formatted hard disk	Loss of data and software, system unusable, disruptions	None
Missing files	Loss of data, disruptions	None
Modified records	Loss of integrity	None
Inaccessible or irretrievable files	Loss of data leads to service disruptions	None

Process 3 identified infrastructure vulnerabilities by examining weaknesses in the hardware, software and systems being used in CISs in each school. The major vulnerabilities were then noted through data analysis and interpretation. Activities carried out in Process 3 concluded major data collection. Information from Processes 1, 2 and 3 was then used to conduct risk analysis and developing protection strategies and mitigation plans, discussed in Process 4.

7.9. PROCESS 4: CONDUCT RISK ANALYSIS AND DEVELOP PROTECTION STRATEGIES AND MITIGATION PLANS

Activities performed in this process were intended to identify, analyse and evaluate risks to critical information systems assets. It also examined protection strategies and mitigation plans that schools could implement to safeguard the critical information systems assets utilising the resources available in view of the identified risks.

7.9.1. Activity 8: Identifying and analysing risks

Threats/threat sources and vulnerabilities to CISs' critical assets were identified in the previous sections. In this activity collaborative teams identified, analysed and evaluated risks most likely to arise from the observed threat/threat sources and vulnerabilities. To achieve this, the impacts of threats and their likelihood of occurring were evaluated using qualitative measures of impacts and their likelihood of occurrence. The qualitative measures were then used in populating a qualitative risk analysis matrix in 7.9.1.1.3, Table 7.16.

7.9.1.1. Evaluating impacts of threats and the likelihood of their occurrence

The initial step to risk identification and analysis involves evaluating impacts of threats or vulnerabilities in a critical asset to the mission and objectives of an organisation (Alberts & Dorofee, 2003). This is followed by establishing the likelihood of a threat exploiting an existing vulnerability in a critical asset. By utilising qualitative measures of the consequences/impacts and likelihoods instead of quantitative measures (probabilities) collaborative teams were able to evaluate impacts of threats to critical assets.

7.9.1.1.1. Qualitative measures of consequences/impact

The impact on the school's operations (productivity), financial loss or reputation (publicity) damage should vulnerability be exploited by a threat was rated using a qualitative scale independently used by Baino (2001), Elky (2006) and Renfroe and Smith (2011) shown below:

- **High impact** – Threats exploit vulnerabilities leading to a significant security breach that could result in operational (productivity) or financial loss or reputation damage to the school;

- **Medium impact** – Threat exploitation of vulnerabilities that could result in some damage or unavailability (denial of service) of a critical asset;
- **Low impact** – Threat exploitation of vulnerability that could result in the disclosure of information about the internal network structure, systems or sensitive information stored in an asset or in transit.

7.9.1.1.2. Qualitative measures of likelihood

The likelihood associated with a particular risk occurring was determined as a combination of vulnerabilities present less the controls implemented to block these vulnerabilities or threats from manifesting into risks (Axelrod, 2003). The scale used for rating was qualitative and is stated below:

- **High likelihood** – a vulnerability was well known, could be exploited using tools or techniques that were publicly available that required little technical knowledge or experience (Axelrod, 2003; Baino, 2001);
- **Medium likelihood** – a vulnerability was difficult to identify, and required some degree of research to resolve or customisation of tools or techniques (Axelrod, 2003; Baino, 2001);
- **Low likelihood** – a vulnerability that required a high degree of technical knowledge or experience, or utilise tools and techniques that are not readily available to most intruders (Axelrod, 2003; Baino, 2001)

7.9.1.1.3. Qualitative risk analysis matrix

A risk matrix is a combination of the consequences/impact rating and the vulnerability exploitation rating qualitatively determined by risk assessors (Axelrod, 2003, Baino, 2001, Renfroe & Smith, 2011). The level of risk was determined by analysing the qualitative values assigned to the resulting impact of threat and the likelihood of threat's occurrence. The risk level determination was performed by assigning a risk level based on the combination of the assigned impact and likelihood levels. The risk-level matrix was created using qualitative measures of the resulting impact of a threat occurrence and qualitative measures of the likelihood of threat occurrence. The matrix was then populated using a high, medium and low rating system. The risk level matrix was then used in determining risk levels in critical assets. Table 7.16 shows the qualitative risk analysis matrix used in this study.

Table 7.16: Qualitative risk analysis matrix or level of risk

	LIKELIHOOD		
CONSEQUENCES	Low	Medium	High
High	M	H	H
Medium	L	M	H
Low	L	L	M

Key: H: high risk, M: medium risk, L: low risk

Sources: Axelrod (2003) and Baino (2001)

This study identified and analysed risks according to three security areas namely organisational, infrastructure/technology and application-specific risks. Each category of risks is briefly discussed below.

7.9.1.1.3.1. Organisational risks

Organisational risks considered in this research study were:

- *user personal security:* risks arising from users' deficiencies in information security;
- *user training in information security:* risks due to the inability of users to cope with current trends in information security;
- *information security policy:* risks that arose from the schools' lack of information security policy that defined different types of information and regulating its use; and
- *physical security* policy: risks arising from the inability of schools to provide adequate physical protection of critical information systems assets.

7.9.1.1.3.2. Infrastructure risks

Infrastructure or technology risks relate to security principles identified by Baino (2001), Renfroe and Smith (2011) and Taylor, Alexander, Finch and Sutton (2008):

- **authentication:** ensuring that only authorised personnel were able to access the CISs;
- **intrusion:** ensuring that access to CISs was only gained through authorised access methods;
- **authorisation:** ensuring that access to the CISs and information was restricted to those with an authorised requirement for such access;
- **encryption:** protecting information in transit and in storage through the use of encryption;
- **accountability:** Ensuring that access to CISs by users was appropriately recorded;

- **availability:** Ensuring that critical information systems assets were available to authorised users all the time;

7.9.1.1.3.3. Application-specific risks

These risks applied to the following specific areas unique to secondary schools situations:

- CASS marks database risks
- Custom application software risks
- User administration related risks
- Operational risks
- Computerised financial information risks

A comprehensive list of risks for both schools was compiled and the results of risk analysis made. The results of the analysis are on Table 7:17 below. These results indicate that there were many risks to CISs' critical assets. The results also show that there were hardly any controls besides expired anti-viruses in some few cases. Risks to critical assets that emanated from this exercise were then evaluated in order to produce a risk treatment priority list. The risk priority list was needed to guide the collaborative teams in making decisions on which:

- risks needed immediate mitigation;
- protection strategy to implement for each critical asset; and
- mitigation strategies needed to be implemented on selected risks.

Table 7.17: Summary of risks in school CISs

Risk item	Critical Asset affected	Threat outcome (Risk)	Control in place	Impact	Likelihood	Relative risk
ORGANISATIONAL RISKS						
Lack of user personal security and training	Information	Destruction or modification - availability or integrity compromised	No control	High	High	High
Lack of information security policy	Information	Theft, modification and destruction - availability and integrity compromised	No control	High	High	High
Lack of physical security policy	Hardware, backup media, information	Theft or destruction of hardware, modification of information	No control	High	High	High
INFRASTRUCTURE OR TECHNOLOGY RELATED RISKS						
Operating system related risks	Custom software	Crashes – loss of availability	No control	High	High	High
	CASS marks database	Data corruption - Loss of integrity	No control	High	Medium	High
Server-computer access permission	CASS marks	Deletion, modification or disclosure	Shared password	High	High	High
Secured resources availability risks	CASS marks	Visible over the LAN -deletion, theft or modification	No control	High	High	High
Lack of access control to computers	All information in computer files	Deletion or modification	No control	High	High	High
		Exposure	No control	Medium	Medium	Medium
Denial of service	Custom software	Unavailable	No control	High	Medium	High
Lack of security incident	All information on	Destruction, modification	No control	Medium	Medium	Medium

Risk item	**Critical Asset affected**	**Threat outcome (Risk)**	**Control in place**	**Impact**	**Likelihood**	**Relative risk**
handling policy	computers/ media					
Malware software protection	Critical information in computers and software	Corruption, Deletion	Expired antivirus software	High	High	High
Power cuts or surges	Hardware	Destruction	No control	High	Medium	High
Theft of accessories	Hardware	System unavailability	No control	High	Medium	High
Security procedures for new users' risks	Hardware & information	Theft, modification, destruction or exposure	No control	Medium	Medium	Medium
Unsecured hubs	Network	Unavailability of connectivity	No control	High	High	High
APPLICATION-RELATED RISKS						
Custom software and Learner CASS Database						
Custom software easily uninstalled, deleted, viral infected	Custom software CASS mark Database	Unavailability	No control	High	High	High
Software incompatibility	Custom software	Unavailability due to system crashing	No control	High	Medium	High
Shared custom password	CASS marks database	Modification – integrity loss	No control	High	Medium	High
		Disclosure	No control	Medium	Medium	Medium
Custom software unable to validate data	CASS marks	Data integrity compromised	No control	Medium	Low	Low
Final marks wrongly	School reports	Data integrity	No control	High	Medium	High

Risk item	**Critical Asset affected**	**Threat outcome (Risk)**	**Control in place**	**Impact**	**Likelihood**	**Relative risk**
computed						
CASS database visibility on LAN	Learner marks record	Destruction	No control	High	High	High
		Modification	No control	High	High	High
		Exposure	No control	High	Low	Medium
Financial process risks						
Unsecured computer system	Financial information	Theft of hard disks	No control	High	Low	Medium
Unsecured accounting system	Financial records	Destruction	No control	High	High	High
		Modification	No control	Medium	Medium	Medium
		Theft or exposure	No control	High	Low	Medium
Payments being disputed	Financial information	Integrity	No control	High	Low	Low
Unauthorised payments		Modification	No control	High	High	High
Multiple payments		Integrity	No control	High	Medium	Medium
Payments not updated on time		Integrity	No control	Medium	High	Medium
Operational risks						
Inaccurate data capturing	All data capturing applications	Data integrity	No control	Medium	Medium	Medium
No authorisation or review for changes	All editable data in the computer	Data integrity	No control	High	Medium	Medium

Risk item	**Critical Asset affected**	**Threat outcome (Risk)**	**Control in place**	**Impact**	**Likelihood**	**Relative risk**
Unavailability of network	Networked applications	Availability	No control	High	High	High
User administration related risks						
Unauthorised changes to system configurations	All information	Integrity	No control	High	Medium	Medium

Alberts and Dorofee (2003) advise that when OCTAVE-small methodology is used to assess information security risks only the impacts of identified risks have to be evaluated. Appendix 5 shows OCTAVE-small risk impact evaluation criteria used to determine the risk priority list. Table 7.18 is a risk priority list with regard to risk impacts and the urgency with which they should be treated. The impact area in which risks were likely to be experienced were reputation of the school, confidence of parents, learners and creditors, productivity and financial loss.

Table 7.18: risk priority in CISs

Critical asset	Risk identified	Impact area	Impact	Recommendation
Custom software	Non availability due to deletion, uninstallation , malware attack	Reputation Confidence Financial loss Productivity loss	High High High High	Treat risks as a matter of urgency
CASS Database	Non availability Destruction Modification	Productivity Financial loss Reputation	High High High	Treat risks as a matter of urgency
Financial Records	Non availability Destruction Modification Exposure	Productivity Financial loss Reputation Confidence	High High High High	Treat risks as a matter of urgency
Computer hardware	Theft Destruction	Productivity Productivity	High High	Risk require urgent attention
Network/ bandwidth	Non availability Hardware theft	Connectivity Productivity	High High	Risk require urgent attention
Educator information	Deletion Modification Exposure	Integrity Confidence	Medium Low Low	May not require immediate attention but need treatment

The priority list, Table 7.18 indicates that most identified risks to critical assets needed urgent attention if the CISs were to remain productively functional. After risk evaluation, collaborative teams developed mitigation strategies for the identified risks.

7.9.2. Activity.9: Developing protection strategies and selecting mitigation plans

In this activity, collaborative teams were engaged in two crucial activities namely developing protection strategies and selecting mitigation strategies.

7.9.2.1.Developing protection strategies

A protection strategy defines the strategies that an organisation uses to enable, initiate, implement, and maintain its internal security (Alberts & Dorofee, 2003). The principal objective of a protection strategy is to provide a direction for future information security efforts instead of finding an immediate solution to every vulnerability and concerns (Alberts & Dorofee, 2003). An organisation's protection strategy leads to a succession of steps that an organisation can take to raise or maintain its existing level of information security. In this study, collaborative teams examined existing protection strategies each school implemented basing on security controls being enforced. The main protection strategy for CISs assets in schools was based on physical security, namely burglar barred doors and windows.

The proposed protection strategy focused on improving the security posture of the schools with regard to CISs critical assets. Table 7.19 shows the strategic area and the proposed security strategy.

Table 7.19: Summary of proposed organisation protection strategy

Organisational protection strategy	
Strategy Area	**Strategy**
Security awareness and training	Introducing baseline information security training to all users of CISs in both schools; Providing basic training in physical security to all users of information systems asset regardless of their job description; Using cheap and readily available information security-training material
Information security strategy	Utilising the outcome of this risk management exercise and the personnel involved in the research to help schools with information security management. School management should be actively involved in implementing of recommended information security improvement measures.
Information security risk	School management should clearly define user roles and responsibilities and communicate these in writing to all personnel.

Organisational protection strategy	
Strategy Area	**Strategy**
management	Administrative educators to prepare an information security status report monthly.
Security regulations	Administrative educators should enforce security regulation to all areas related to CISs. School management should sanction users who violate information security rules
Disaster recovery plan	Draft contingency plans and procedures for disaster recovery that all users of CISs clearly understand and able to implement
Physical security	Put in place enforceable physical security procedures that empower security guards to perform thorough spot checks for moveable information systems assets. Develop enforceable regulations on workstations used for administrative purpose. Specify physical security requirements for computers in administrative offices in with respect to their usage requirements. Enforcing software installation security procedures to all users of computers and ensure they are adhered to by all staff members in the schools. Clearly specify an individual responsible for software installation, computer configurations and hardware movement. Installing video cameras in the main building where most information assets are stored.
Information technology security	Establish clear procedures for information technology security services. Encrypting all sensitive information stored in computer storage media. Introduce user access rights to restrict access to sensitive information. Enforce user password policies that stop sharing of passwords by users Enforce user logoff during short breaks or time-off on all workstations used for administration purposes.
Security staff	Schools address incidence management by documenting clear techniques and reporting mechanisms for incident identification and reporting.

7.9.2.2. Selecting risk mitigation plans

Risk mitigation plans are intended to reduce the risks to critical assets (Alberts & Dorofee, 2003, Panda 2009). The main focus of risk mitigation plans for this research was CISs' critical assets. The mitigation plans were specific to the risks associated with the information systems' critical assets found in secondary schools. The suggested mitigation plans were within each secondary school's human and financial resources means. A number of factors influenced the selection of risk mitigation plans namely:

- identified threats/threat source or vulnerabilities and their risk impact;
- controls or control required to offset the risk or protect critical asset;
- the complexity of implementing the controls considering the technical abilities of the participating members from each school;
- the cost of implementing such controls in regard to financial resources of the school;

A summary of proposed mitigation plans for each critical asset is presented on Table 7.20

Table 7.20: Mitigation plans for critical assets

Threat Type	Actions
CASS marks database risk mitigation plans	
Users using network access	Enforcing password discipline and reporting password abuse; Changing passwords on computers and databases regularly; Restricting access to a shared folder that contain the database files; Identifying the users who access the database and assigning access privileges; Database access by other computers should only be through custom software; Encrypt all marks in the database
Users using physical access	Use different passwords for each computer Activate password protected screen savers as time-out defaults. All CISs users should sign a nondisclosure form Install a camera in the reception to capture unauthorised users who sneak in during awkward times
System problems	Upgrade system hardware and software components on regular basis. Reconfigure computers and software for optimum user support. Configure restore points to suitable dates for system restoration Use genuine software from licensed vendors Restrict unauthorised software installations Uninstall all conflicting software from all computers with critical information

Threat Type	Actions
Malware	Educate users on preventing viruses from being introduced into systems. Install a trusted antivirus/antispyware and always update the antivirus Install operator screen notification of virus activity. Configure computers to automatic antivirus update and viral scans Configure the server-computers to stop it from accessing the world-wide-web Restrict installation of software by users on their workstation by giving all users limited privileges
Measures	Provide compulsory training in basic security awareness for staff members who use computers in schools Conducting compulsory training in malware scanning and cleaning.
Custom software risk mitigation plans	
Users using physical access	Create user passwords for the custom software. Disguise the software icon on the desktop Always close the application when going out for breaks Disable mark editing and report printing features on peripheral computers.
System problems	Upgrade operating systems with most recent patches Uninstall incompatible software from all computers that run this software Renew license on time to avoid crashing and shutouts on expiration
Malware	Run up-to-date antivirus programs that are compatible with the custom software Empty antivirus vaults regularly
Personal computers risk mitigation plans	
Users using network access	Disable file sharing on all other computers including server-computers Configure network password for computers used in school administration in addition to individual computer passwords. Disable guest user account on all computers used in the school administration Remove profiles of users who fail to comply with security policy requirements.

Users using physical access	All unattended workstations should run password protected screen savers or require passwords from hibernating. Physically secure all computers and accessories to deter unauthorised movement. Reviewed physical security of all computers used in CISs Close all windows to the offices where important computers are found
System problems	Introduce PC disaster recovery plan in the event of power cuts or surge. Use UPs and power surge protector on the server-computers Switch off all computers at the end of the day on daily basis.
Financial accounting information risks mitigation plans	
Users using network access	Remove computer from the network.
Users using physical access	Computers should be accessed by Financial educator only. Password-protected computers
System problems	Practice regular software update Make backup and store it in separate rooms
Malware	Avoid use of removable storage media from free flow computers Install most recent virus detection software Perform malware scans regularly
Measures	Report status for this plan on a monthly at meetings.
Network infrastructure mitigation plans	
Human actors using physical access	Secure the router and the hubs to prevent theft or illegal exchange Restrict access to the router by all unauthorised users
System problems	Isolate hubs from kitchen utensils plugs to provide continuous connectivity problems
Other problems	Use network passwords to prevent illegal connections to WLAN Remove unused data cables plugged in the hubs in all offices Secure all dangling data cables

Information on Table 7.20 shows a number of mitigation plans that were proposed. Most of the mitigation plans were within the level of skills of the individuals who were in charge of the computerised information system. Effort was also made to suggest cheap and easy and implementable plans.

7.9.2.3. Information security risk treatment

Risk treatment involves the selection and application of the most appropriate risk security controls or controls intended to modify the identified risks in order to avoid possible damages to critical information systems assets (Hoo, 2006; Shortreed, 2008). In this study, three risk treatment strategies were adopted based on the severity of the impact of the risk on the critical asset, namely risk avoidance, risk acceptance and treating the risk. These strategies were discussed in detail in Chapter 4 of this study, 4.3.3. Some treatment strategies required controls to be put in place. Table 7.21 shows the results of the risk treatment used in this study.

The results of risk treatment on Table 7.21 show that schools chose to treat the risks and apply preventive, detective, deterrent or corrective controls to alleviate risks to their CISs critical assets. Collaborative team members were given opportunities to use the tools for security control and were also taught how to configure passwords on computers and files. However, use of passwords on files remained a contentious issue as some users felt that they were likely to forget the passwords resulting to inaccessibility of the information in the affected files.

Table 7.21: Risk Treatment results

Threat source /vulnerability	Risk	Impact	Treatment applied /recommended
Unauthorised users access the CASS database over the network	Modification of data leads to loss of integrity Deletion of data files leads to loss or disruption of productivity. Reputation of schools was under threat.	High	- Avoidance – Disabled list folder contents of the folders with CASS databases on the server-computers so that unauthorised users will not see the CASS database - Preventive controls- segmented the LAN into two and used network password to prevent unauthorised access to all administrative computers - The WLAN access code was reset from default to user defined.
Authorised users access CASS database using the network	Modification of marks compromises integrity, Deletion of files compromises availability and productivity	High	- Preventive controls - Except for the Administrator-educators, the modify privilege was disabled for all other authorised users to stop them modifying records.
Unauthorised users using physical access to computers with CASS database and financial information	Modification of marks – integrity was compromised. Modification of financial records – wrong payments leading to financial loss by schools	High	- Preventive controls – Access user passwords were set to standard user on all computers. Files containing sensitive information were also password protected. Recommended zoning of critical assets, no unauthorised person to be allowed to use critical information systems assets.
Authorised users using physical access to computers with CASS database and financial	Modification of marks Deletion of files Exposure of sensitive	High	- Preventive controls – enforced user authentication and authorisation. Disabled the guest account - Deterrent controls –locking out users who misuse passwords

Threat source /vulnerability	Risk	Impact	Treatment applied /recommended
information	information		
Persistence crashing of custom software	Disruptions /loss of productivity as availability is compromised (denial of service)	High	- Corrective controls – frequent updating of the operating systems with relevant patches. Systems should be able to recover from these crashes - Preventive controls – renewing software licences on time system - Detective controls – Activate alerts to warn users about pending crashes
Sharing of single password to access custom software	Unaccounted data modifications of deletions	High	- Preventive controls – user should have own password to the custom software. - Detective controls – these warn the Administrative educator of possible attempts of logging using unauthorised login details on server-computer.
Infection of computers by malware	Corruption of data files and software leads to denial of service	High	- Preventive control – installing trustworthy malware software - Detective control – updating existing malware to detect new malware
Theft of computer hardware or accessories or unauthorised disconnections (hubs, hard disks)	Loss of information Loss of connectivity Productivity severely affected	Medium	- Preventive controls – physical securing the accessories so that they cannot be removed easily. Use surveillance cameras in rooms with these assets
Power surges	Destruction of hardware leads to loss of information	Medium	- Preventive controls – installing UPSs to all administrative computers.

7.10. CONCLUSION

This chapter gave a detailed account of a qualitative case study on information security risk management in CISs conducted in two selected secondary schools. The case study was based on the OCTAVE-small risk management methodology. Data were collected using participatory observation, inspection checklists, interviews and customised OCTAVE-small worksheets. Data were gathered on security practice, threats and vulnerabilities of critical information systems assets. Major data sources were collaborative team members (users), school managers, information systems assets and the environment in which they were used. Collaborative teams participated in data collection, discussions during and after each data collection activity and demonstrations using computing technology. Only qualitative data were gathered, then qualitatively presented, analysed and interpreted. Threats and vulnerabilities in CISs assets were identified, impact of these threats and their likelihood were determined qualitatively using a risk level matrix. Risks were then identified and analysed, leading to the proposal of protection and mitigation strategies. The conclusion to the chapter reflects on the key issues of data collection, presentation, analysis and interpretation.

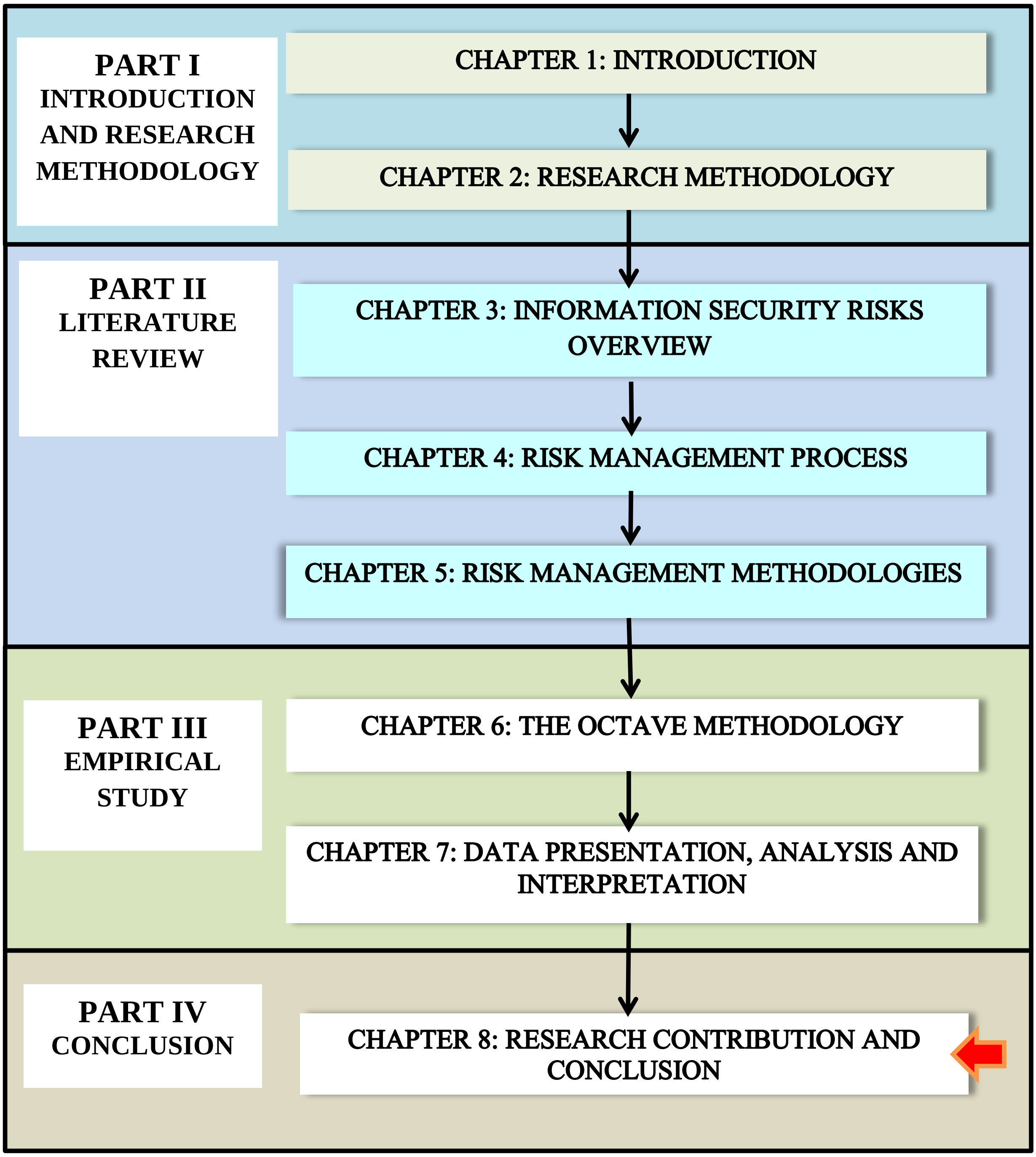
The next chapter, Chapter 8 discusses findings, conclusions, makes reflections and recommendations for further studies.

PART IV

RESEARCH CONTRIBUTION AND CONCLUSION

CHAPTER 8

8. RESEARCH CONTRIBUTION AND CONCLUSION


PART I
INTRODUCTION AND RESEARCH METHODOLOGY
CHAPTER 1: INTRODUCTION
CHAPTER 2: RESEARCH METHODOLOGY
PART II
LITERATURE REVIEW
CHAPTER 3: INFORMATION SECURITY RISKS OVERVIEW
CHAPTER 4: RISK MANAGEMENT PROCESS
CHAPTER 5: RISK MANAGEMENT METHODOLOGIES
PART III
EMPIRICAL STUDY
CHAPTER 6: THE OCTAVE METHODOLOGY
CHAPTER 7: DATA PRESENTATION, ANALYSIS AND INTERPRETATION
PART IV
CONCLUSION
CHAPTER 8: RESEARCH CONTRIBUTION AND CONCLUSION

8.1. INTRODUCTION

The main objective of this research study was to assist secondary schools that used CISs to develop a set of guidelines they would use to effectively manage information security risks in their computerised information systems. In this qualitative case study, data on critical assets, threats, vulnerabilities, security practices and controls in CISs in each secondary school was collected using a variety of instruments. This study analysed and assessed information security risks in critical information systems assets using the OCTAVE-small risk management method. Two secondary schools were involved in this case study in which users of the CISs took part in the risk management exercise to gain information security knowledge and skills required for future use. The outcomes of this research study were CISs users who appreciated information security risks and set of simple and easy to implement information security guidelines.

Up to this point, seven chapters have been meticulously compiled focusing on related information security risks in information systems. The previous chapter, Chapter 7 implemented the OCTAVE-small method in data collection from school managers, users, CISs assets and the environment in which these assets were used. Qualitative data were collected using participatory observation, physical inspection and interview methods in which observation schedules, inspection checklists, interview schedules and customised OCTAVE-small worksheets were used as data collection tools. Data were presented in tabular and dump screen formats. Analysis was qualitatively done in the form of textual narrations and descriptions supplemented by extracts from interview transcripts.

The purpose of this chapter is to provide a research overview which states and briefly discusses the findings of the research study and provide a conclusion based on these findings. The chapter further reflects on the educational value of the research to the schools that participated in this study and other secondary schools in the same situation and suggests areas of further research.

The structure of this chapter is as follows: an introduction that gives the purpose of the chapter, research overview that discusses findings based on research objectives, contribution of the study, conclusion, recommendations and further study.

8.2. RESEARCH OVERVIEW AND CONTRIBUTION

The main objective of this research study was to assist secondary schools that used CISs to develop a set of guidelines they would use to effectively manage information security risks in their computerised information systems. To achieve this, three sub-objectives stated in Chapter 1 provided guidelines for the study. The sub-objectives were explored in various chapters of this document and are further examined here to establish the extent to which they were achieved. Each of the following subsections explores a particular objective. Findings made by this study are stated under the respective sub-objective together with brief discussions.

8.2.1. Sub-objective 1 – Systematically gather data on critical assets and information security controls in CISs of two secondary schools

The first objective of this study was explored in Chapter 3 subsection 3.4. The chapter surveyed literature on a variety of information systems assets and categorised them as critical and non-critical depending on the importance of the operations each asset supported in an organisation. Critical information systems assets found in small-scale organisations were also presented on Table 3.1. The finding of this research on critical information systems assets was consistent with those identified by Microsoft TechNet (2006), as discussed in Chapter 3. Secondary schools' CISs consisted of many critical assets that required protection. Table 8.1 is a summary of the identified CISs critical assets found in secondary schools which needed protection against a variety of risks.

Table 8.1: Summary of critical assets in secondary schools

Critical asset	Category	Uses
CASS marks database	Information	Stored all marks and reports per term used for individual learner's progress and yearly promotions
Custom application	Software	Used to capture marks, process mark schedules, reports and statistics for use by schools and education authorities
Financial records and information	Information	Creditors' records, school fees, salaries of part time workers and payment records, government support funds
Computers and software	Hardware and software	Used in the administrative offices to store critical information.
Modems and hubs	Hardware	Provided internet and LAN connectivity to all

Critical asset	Category	Uses
		computers in the schools
Educators personal information and salaries	Information	Used to create educators' profiles at school. The information included academic qualifications, educators' reports from heads of departments used for quality control, promotion, subject allocation and monthly salary processing.

These critical information systems assets supported a variety of important operations in secondary schools and this underscored the importance of securing them from threats. The purpose of sub-objective 1 was to identify critical assets in CISs in secondary schools. Upon achieving this objective, the researcher proceeded to identify information security controls that secondary schools implemented to protect the identified CISs critical assets. The following sub-section discusses the forms of security controls used by schools to protect CISs critical assets.

Chapters 3 and 4 also discussed information systems protection mechanisms that small-scale organisations could implement to secure their information systems against impending risks. In Chapter 7, secondary schools' CISs were inspected to determine security protection mechanisms being implemented. It was found that the only protection mechanism that secondary schools relied on was physical security of computer hardware and accessories. This was achieved by using burglar-barred doors and windows intended to prevent or deter unauthorised access and theft of computer hardware especially during nights and school holidays. Physical security concerns itself with threats, risks, and controls to protect facilities, hardware, data, media and personnel (Hansche, 2001; Caballero, 2009). The ISO 17799 (2000) stipulates that computing equipment should be physically protected from security threats and environmental hazards. Inadequate physical security to critical information systems infrastructure and information resources in both secondary schools implied that the assets were exposed to various threats. By providing adequate physical security to their CISs critical assets, secondary schools would be able to restrict physical access to these assets only to authorised personnel who needed access to perform authorised functions and operations. Secondary schools failed in this regard as evidenced by unauthorised movement of computer hardware by different users.

There were no protection mechanisms for data and software in both schools. This was a clear indication that school managers and users of CISs were mainly concerned with computer hardware instead of data and information that were stored in their computers. There were also deficiencies in technical security systems concerning antivirus, antispyware software and firewalls. In order to determine the implications of these deficiencies, a risk assessment and analysis exercise using OCTAVE-small method was conducted as indicated by sub-objective 3. Subsection 8.2.3 discusses findings of the risk assessment and analysis performed in the two secondary schools.

8.2.2. Sub-objective 2 - To identify an easy to use risk management methodology that non-technical personnel in secondary schools can utilise

This objective was underpinned by discussions in chapters 4, 5 and 6. Chapter 4 discussed risk assessment and analysis in general. Chapter 5 elaborated on quantitative and qualitative risk assessment and analysis methods emphasising on their differences along with strengths and weaknesses in their implementation by small-scale organisations. Chapter 6 examined OCTAVE-small method and its implementation in small-scale organisations like secondary schools. The OCTAVE-small method was then implemented in Chapter 7 in which data were collected using a blend of risk management methodologies such as participatory observation schedules, inspection checklists, interview schedules and customised OCTAVE-small worksheets.

The following sub-sections delineate and emphasise findings of this research study that show the extent to which this sub-objective was achieved.

8.2.2.1. Organisational security practice

It was observed that secondary schools lacked proper organisational security practices and as a result, CISs assets were accessed and used in the manner determined by users thereby making these assets highly vulnerable to a number of threats. Poor organisational security practices emanated from lack of information security policies related to physical security, personal security awareness and training, access control, disaster recovery plans, and virus and malware policies. Lack of security policies on utilisation of information systems assets is detrimental to the organisations as both inside and outside users attack the critical information that has taken time for an organisation to accumulate (Cappelli & Moore, 2008). This situation prevailed in the secondary schools where the research was conducted. It was also observed that managers and users of CISs were not concerned about the manner they used critical information systems assets as long as computers were working.

8.2.2.1.1. Lack of information security policy

Lack of information security policies in secondary schools made it difficult for managers to clearly determine how CISs assets could be used responsibly while being protected. Information security policies were required to highlight restrictions to the disclosure, modification, availability or use of critical information in an organisation (Canavan, 2001; Doherty & Fulford, 2006; Taylor *et al.* 2008). In secondary schools, no one was accountable or held responsible for any misuse or abuse of information systems assets due to lack of such policies.

8.2.2.1.2. Uncontrolled access to critical information

Secondary schools were unable to identify and separate their critical and sensitive data or information from less sensitive data. This had implications on storage and access to data/information by various users of the CISs. Schools unknowingly made all information available to the public over their LANs. This facilitated unauthorised access to most of their critical information over the LANs. By connecting and implementing networks, secondary schools had an obligation to take some precautions to reduce the risk of unauthorised access to the critical information assets. Information systems users often engage in risky behaviours that threaten the security and integrity of the organisation by exposing sensitive information or weakening the existing technological perimeter security (Hansche, 2001; Cox, 2012). The risk behaviours by some CISs users were either deliberate or accidental, but either case had the potential to cause severe damage to secondary school reputation, finances and to potentially harm learners.

Computerising information systems in secondary schools seems to have increased direct access to all confidential information by authorised and unauthorised users. The critical information in these schools was being accessed through unauthorised manner and unauthorised modifications performed on it as alluded to by interviewees in Chapter 7. There was loss of integrity and confidentiality through modification and disclosure of confidential information. All forms of information security violations and breaches by users were potentially damaging secondary schools' reputation, financial resources and learners' confidence.

8.2.2.2. Security requirements for critical information systems assets

A set of security requirements for critical information systems assets for secondary schools' CISs were identified and are listed on Table 8.2.

Table 8.2: Critical assets' security requirements

Critical asset	Most important security requirement
Learners CASS marks database	Integrity, availability and confidentiality
Custom software	Availability
Financial information	Integrity, confidentiality and availability
Computers	Availability information resources
Routers and hubs	Availability of connectivity
Educators personal information and salaries	Integrity, confidentiality and availability

Secondary schools participating in this case study did not provide the basic security requirements for their CISs critical assets besides physical security protection. This left the critical assets severely exposed to threats.

8.2.2.3. The main threats to CISs critical assets

The main threats to critical assets were authorised and unauthorised users, malware, system crashes, errors, access path to critical assets and information security breaches.

- *Authorised users* deliberately modified or stole critical information from computers they used. In some cases the users deliberately deleted critical information to delay or stop important processes from taking place. Authorised users also accidentally infected computers with viruses from removable media they used outside school. Some authorised users deliberately formatted or removed hard disks from computers without backing up critical data and information. This posed as a major threat to critical information stored in computers;
- *Unauthorised users* also deliberately modified, deleted or disclosed critical information for various reasons, including embarrassing managers, disrupting

certain operations or for financial gains. These users were also found to be responsible for removing or replacing hubs, illegal connections of personal laptops to the LANs;

- *Malware* (viruses and Trojan horses) either from the Internet or externally used removable media such as memory sticks were also a major threat to data, information and system software. Malware found on many computers was reported to be causing havoc by corrupting, deleting, hiding or locking files containing critical information.
- *System crashes* due to software conflicts, missing patches and operational environment were also prevalent making data capturing and processing difficult;
- *Errors* in the custom application frequently produced school reports with wrong computations and final grades. Incorrect examination results analyses output generated by the custom application damaged school management's reputation as local education authorities, parents and learners expected better quality services from these schools.
- *Access paths to critical information* provided an unauthorised means by which critical information assets could be accessed by users within schools. School managers and administrative educators were ignorant of the existence of these access paths and unauthorised access to critical information. Illegal connections through the Ethernet LANs provided easy access to shared folders and files on server-computers. These did not require access passwords and were difficult to detect. Workstations in administrative offices which were left unattended also provided easy access to critical information. Unauthorised users capitalised on the unsecured workstations to modify or print critical information in the absences of the office bearers. Unauthorised users also capitalised on unsecured LANs to gain access to the administration computers and then launched surprise attacks. These used free data cables or extra ports on the hubs or unsecured wireless connections to achieve these malicious acts.
- *Information security breaches* were committed deliberately or accidentally by authorised and unauthorised users of CISs who capitalised on existing vulnerabilities. During interviews, users alluded to situations where the information they used was deliberately changed by other users. The main breaches targeted the CASS marks and financial information. There were strong claims that

some inside users stole or modified certain information for financial gains. It was also noted that unauthorised inside users used critical assets in a way that was intended to harm the schools or individual managers. In some cases stolen financial records were used to discredit school managers during meetings.

8.2.2.4. Information security risks

It was found that CISs critical assets were exposed to risks such as organisational risks, infrastructure (technological) related risks and application-related risks. The levels of these risks were generally high and impacted highly negative on the CISs, hence school operations and reputation. High impact *organisational risks* were due to lack of important policies such as information security policy. *Infrastructure-related and application-related* risks were due to defects in hardware, errors in custom application, incompatibility between custom application and operating systems of recent versions, missing operating system patches or registry issues. These vulnerabilities led to unavailability, loss of integrity and compromise in confidentiality of the critical information that secondary schools relied on for their operations. This caused secondary schools to suffer negatively in terms of productivity, reputation and financially.

In this subsection, a variety of information security risks to CISs were identified through a simple risk assessment and analysis exercise, as a result of this, secondary schools were expected to put in place controls to these risks. One of the objectives of this study was to suggest generic mitigation strategies that these secondary schools could implement to alleviate the identified information security risks. Subsection 8.2.4 elucidates a number of generic information security mitigation strategies within the means of secondary schools human resources and financial capabilities.

8.2.3. Sub-objective 3 - To deduce generic guidelines that could be followed during information security risk management at a secondary school that take into account CISs users who were not experts in risk management.

Risk mitigation strategies were discussed in Chapter 4. The conventional risk mitigation strategies tend to be technical in nature and difficult to be implemented by CISs users in secondary schools. Such strategies ignore the role played by CISs users in improving information security status in small-scale organisations (Panda 2009). The main objective of this research study was to assist secondary schools that used CISs to develop a set of guidelines they would use to effectively manage information security risks in their computerised information systems. These guidelines were intended to help schools implement protection and mitigation strategies that emphasised the active participation of CISs users. Besides addressing standard problems, the protection and mitigation strategies addressed problems peculiar to schools' CISs. This research study developed a set of guidelines that recommended various protection and mitigation strategies intended to improve the security of critical assets taking into account the level of skills of the personnel responsible in carrying out these tasks. The protection and mitigation strategies required that:

- schools develop enforceable information security policies to govern the use of CISs and other computing facilities;
- all users of CISs and other users of computers be trained in basic information security and awareness;
- all computers in the school used in CISs be removed from the main LAN and placed in their own segment;
- all computers be password-protected;
- each school appoints an educator to implement the information security policies
- schools install antivirus and antispyware suite on all computers and carry out regular updates
- schools to configure all internal firewalls to high level to restrict unauthorised access to administrative computers by outside computers; and
- schools to perform information security risk management exercises regularly

The following section, 8.3 are discussions emanating from the above overview and that are meant to provide general guidelines that secondary schools can possibly implement with great easy in the management of the risks in their information security risks.

8.3. DISCUSSIONS

Section 8.2 examined the overview of the research study and detailed the findings as per objectives. This section examines various strategies that were found to be applicable to secondary schools' CISs context.

8.3.1. Protection and mitigation strategies

The levels of risk impact and their likelihood of occurring which are reported in Chapter 7 were high and some threats had already caused noticeable harm on CISs such as rendering the assets unusable, financial loss and damage to school reputation. The suggested protection levels for most identified risks were considered to be medium and mitigation strategies were also based on simple, effective and manageable mechanisms that required active participation of the CISs users and school managers. Threats, vulnerabilities and controls have changed and grown in complexity, however, it was important to consider the easiest and often cheapest controls before considering large or expensive solutions as suggested by Taylor *et al.* (2008). This approach underpins the recommended protection and mitigation strategies that addressed organisational vulnerabilities in information security practices in secondary schools and also technological vulnerabilities in CISs assets. The recommended protection and mitigation strategies were meant to reduce existing risks, detect and prevent threats from utilising vulnerabilities in critical assets and a recovery from threat effects. The information security controls are discussed in next subsections.

8.3.1.1. Organisational protection and mitigation strategies

These strategies were meant to address the manner in which CISs critical assets in secondary schools were accessed and used. This was based on Caballero (2009)'s argument that organisations that focus on the technical attacks and neglect items such as policies and procedures or employee training and awareness were setting information security up for failure. Therefore, the strategies discussed below were meant to have far reaching positive effects on the schools CISs. The strategies were:

- ***Information security policy-*** This study prompted school managers to set information security committees tasked with drafting information security policies. Secondary schools were assisted to develop simple information security policies to address CISs risks. Information security policies were the basis for the dissemination and enforcement of sound security practices within the secondary school context as recommended by Doherty and Fulford (2006). The policies addressed the use of computing facilities, the movement of computer hardware, access control, incident management and penalties associated with violations. This was in line with Williams (2008)'s recommendation that to become the foundation of security culture, information security policy and its dissemination should seek a balance between users' understanding of the threats, effective deterrents and associated penalties.

- ***Basic education and awareness training in information security risk management*** – Previous research studies show that information security objectives can hardly be met by technical and procedural protection only, but by an educated security attitude of managers and employees of an organisation that utilises an information system (Rezgui & Marks, 2008). In order to increase information security awareness among users, Rezgui and Marks (2008) encourage organisations to enforce information security awareness through education and training. In secondary schools, authorised and unauthorised users who intentionally or accidentally breached information security posed as information security threats. Some of the security violations and misuse of critical assets occurred due to information security ignorance on the part of the users. For example, Sarkar (2010) argues that authorised users who commit security breaches do not think that the violations are unethical because they lack the moral inhibitions that are mostly defined by their culture, background and character. This implies that CISs users should not be expected to instinctively protect critical data and information without the awareness necessary to effectively safeguard information (Rezgui & Marks, 2008). Therefore, by encouraging active participation of CISs users in collaborative teams, this study ensured that most key users developed an appreciation and awareness of information security threats and risks in their CISs. The study was also used as a means to attract attention of CISs users and managers to information security risk in their CISs and the need to conduct risk management exercises regularly. Information system security awareness requires users to understand information system security in general and optimally committing to it (Rezgui & Marks, 2008). This study also sought to instil a positive attitude of information security awareness among the users so that they could use the critical assets responsibly to benefit concerned schools. The study also drew the attention of the school managers and users to risks inherent in their CISs and prompted them to act responsibly in securing these assets using sanctioned procedures.

Besides organisational strategies, the study also focused on other security controls which were within the comprehension of the users of CISs in schools. The strategies are discussed in the following subsections.

8.3.1.2. Technical protection and mitigation strategies

The OCTAVE-small risk management method encompasses organisational and technological protection and mitigation based strategies. Technological protection and mitigation strategies emphasise on technical and physical controls of critical assets such as hardware, software and information. Technical controls use software and hardware resources to control access to information and computing systems, to help mitigate the potential for errors and blatant security policy violations (Caballero, 2009). This study encourages secondary schools to implement technical controls which are simple and easy for novice users of CISs. These included antivirus and antispyware software, data encryption, passwords, auto-account logoff, firewalls, systems up-dates and data backups. Each user involved in this study was given an opportunity to be acquainted with each technical control briefly outlined below:

- ✓ ***Installation of antivirus, antispyware and scanning of malware* -** Antivirus and antispyware software are technical controls that detect, identify, prevent and remove malware from a computer system in order to prevent or reduce data corruption, destruction or theft. These offer both detective and preventive defence mechanisms to data and software stored in computer systems. Therefore, there was need to install an antivirus on every computer system within each school. Secondary schools involved in this research study were in dire financial problems and could not afford to buy antivirus and antispyware software. Schools eventually utilised free downloaded ***Anti-Virus Guard (AVG)*** 2013 and Avira. Each collaborative team member was tasked to download and install antivirus and to scan malware from their respective computers. Furthermore, team members were trained on how to update antivirus. Another positive contribution made by collaborative teams was encouraging other educators to bring their laptops or computers for antivirus installations and malware scanning. This enhanced team members' skills and knowledge in information security awareness.

- ***Encrypting and password-protecting CASS marks database* -** Collaborative teams recommended secondary schools to password-protect their CASS marks databases and encrypt all data in order to prevent direct access to this critical asset by both authorised and unauthorised users. Once the data in the database was encrypted, the database would be accessed through the custom application. However, the encryption was to be effected by the custom application developer so that encryption and decryption of data were performed by custom application during data capturing, processing of results and printing of reports. To improve the security of the custom application software, the application developer was asked to introduce access accounts and privileges for different users. Data capturing was to be done by administrative educators while modification of that data could be performed by the deputy principals.

- ***Setting user access rights and auto-account logoff -*** To restrict user access to computer systems, collaborative teams created user access accounts and set access rights. User accounts were created on each computer and each user was allocated relevant access details. The guest account was disabled and the administrator account was used solely for administrative purposes by the educator in charge of CISs administration. This was meant to prevent authorised users from creating rogue accounts which could be used to illegally access the server-computers. Password-protected screen savers and automatic logoff were also activated on all computers to protect data and software from unauthorised users in the event that the authorised users left their workstation unattended.

- ***Firewalls-*** A firewall is a software program or piece of hardware that helps to screen out hackers, viruses and worms that try to reach a computer over the Internet (Rouse, 2007; Bauer, 2012). Most computers in the two schools had their firewalls turned off. Authorised users were trained on the importance of the firewalls and how to configure them. From the onset, all firewalls were turned on and configured as per computer usage.

- ***Systems up-dates -*** Software update plays a critical role in ensuring that organisations keep their computer fully up-to-date with the latest security patches and software updates, without unduly compromising reliability, productivity, security and data integrity (Galea Francheschini Innovation GFI White Paper, 2005). It was imperative for this study to educate and train CISs users in basic software updates. The exercise was performed on most updatable software installed on computers used in CISs. The update exercise included the Windows operating systems, adobe reader and antivirus software. CISs users were able to perform software update checks.

- ***Backup and restore capabilities* -** Secondary schools did not perform regular backups for their critical data and information as there were no policies or measures to compel them to do so. Data backup refers to the copying of data and information stored in computer storage media so that these copies may be restored through data recovery process after some fatal event (Guidance Consulting Inc, 2012). Backups serve two primary purposes namely:
  - *disaster recovery:* to restore a computer to an operational state following an accident;
  - *file or data recovery:* to recover data or information files after they have been deleted or corrupted (Bednash & Halstuch, 2010; Guidance Consulting Inc, 2012).

Prior to this study, critical information had been left vulnerable due to lack of regular backups on which the schools could recover in the event that the original copies were destroyed or corrupted. Only a comprehensive disaster recovery strategy where everything is backed up on a regular basis may have a chance of returning things to normalcy within an acceptable period of time (Mah, 2012). This important security requirement which secondary schools have been overlooking was addressed during the study through collaborative training of CISs users in basic information security. This research study regarded lack of backups as a form of insecurity or vulnerability that was likely to affect school operations in due future. Therefore, there was a need to train CISs users on how to back-up all vital information they were using.

Besides technical protection and mitigation strategies, this study also focused on physical security of the critical assets through implementing a number of physical controls. Subsection 8.3.1.3 is a list of physical controls compiled to assist secondary schools to attain sustainable information security programmes.

8.3.1.3. Physical controls

The following list of physical controls was compiled to help secondary school managers and CISs users to effectively implement these controls to safeguard critical assets they possess.

- ✓ physically securing on tables all computers holding critical information;
- ✓ securing all hubs by locking them in small and immovable steel cages, and removing unused data cables from them;
- ✓ securing data cables on walls;
- ✓ separating networks into two functional areas;
- ✓ protecting the administrative functional area by using network passwords;
- ✓ removing server-computers from the Internet;
- ✓ possibly installing a surveillance camera in the vicinity of the CISs in receptions;
- ✓ separation of roles and duties to ensure that an individual would not complete a number of critical tasks alone;
- ✓ installing physical controls to monitor and protect the physical environment of the workplace and CISs facilities;

This study sought to contribute to information security risk management in secondary schools by providing a set of guidelines that non-technical users could implement in order to manager information security risks in their CISs. Section 8.4 outlines the research contribution made so far.

8.4. RESEARCH CONTRIBUTION

The main objective of this research study was to assist secondary schools that used CISs to develop a set of guidelines they would use to effectively manage information security risks in their computerised information systems. Achieving this objective was the major contribution of this research. This section delineates the research contribution in this specific important area by providing a summary of guidelines that arose from the empirical risk management activities performed in two secondary schools that frequently used CISs. The guidelines were derived from the discussions in the previous section 8.3 of this research study. The guidelines emphasise on the importance of protection and mitigation strategies within reach of secondary schools that utilise CISs. The protection and mitigation strategies were categorised as organisation, technical and physical.

8.4.1. Organisational information security guidelines

These guidelines sought to encourage secondary schools to address the manner in which their CISs critical assets were accessed and used. The guidelines provided the bases on which secondary schools formed their security policies and procedures. They also outlined the need to provide users of CISs with security employee training and awareness. The guidelines required that schools:

- ***Develop viable and implementable school-based information security policy by***
  - ✓ Setting-up school-based information security committees responsible for drafting information security policies commensurate with envisaged risks in respective CISs;
  - ✓ Using information security policies as the basis for the dissemination and enforcement of sound security practices within the secondary school context as recommended by users of CISs;
  - ✓ Applying information security policies to address the use of computing facilities, the movement of computer hardware, access control, incident management and penalties associated with violations;
  - ✓ Using information security policy to instil information security culture among users of CISs in secondary schools; and
  - ✓ Fostering a security culture that balance between users' understanding of the threats, effective deterrents and associated penalties.

- ***Provide for basic education and awareness training in information security risk management to all CISs users and other users of computers in the schools through:***
  - Developing a strong information security awareness and positive attitude among CISs users in order to reduce their overreliance on technical and procedural protection;
  - Information security education and awareness activities that encourage active participation of CISs users in collaborative teams so that they developed an appreciation and awareness of information security threats and risks in their CISs;
  - Instilling a positive attitude of information security awareness among the users so that they could use the critical assets responsibly to benefit concerned secondary schools;

8.4.2. Technical protection and mitigation strategies guidelines

Technical protection and mitigation strategies play a crucial role in CISs of an organisation. Schools tend to lack personnel with skills to implement them. However, this study provides guidelines that secondary schools can implement to offset the problem.

- ***Provision of reliable technical protection and mitigation strategies***
  - ✓ Secondary schools should rely on school-trained CISs users to install antivirus, antispyware and scanning of malware.
  - ✓ Secondary schools should encourage all educators who have laptops or computers to have their gadgets installed with antivirus/malware and scanning.
  - ✓ In the event that an outsider is hired, the school should attach at one of its CISs users to the hired personnel for monitoring purposes.

- ***Encrypting and password-protecting critical information marks database***
  - ✓ Secondary schools need to password-protect their critical information or encrypt all data in order to prevent direct access by both authorised and unauthorised users.
  - ✓ Secondary schools should use authorised software to access their databases.

- ***Setting user access rights and auto-account logoff***
  - ✓ Secondary schools should restrict access to their CISs by unauthorised users creating user accounts and setting access rights to all accounts.
  - ✓ Secondary schools should disable all guest accounts on all computers used in CISs to prevent creation of rogue accounts that could be used to illegally access the critical information.
  - ✓ Secondary schools should activate password-protected screen savers and automatic logoff on all computers to protect data and software from unauthorised users in the event that the authorised users left their workstation unattended.

- ***Stringent use of inbuilt firewalls***
  - ✓ Secondary schools should make sure that all computers used for CISs have firewalls that work properly to prevent unauthorised by external computers.
- ✓ Providing a sound training of authorised CISs users on how to activate and configure firewalls on their computers.

- ***Frequent systems software update***
  - ✓ Secondary schools should perform software update on all computers used for CISs on regular basis.

- ***Practice regular backup for critical information and system restoration***

  This frequently overlooked security measure need to be taken seriously by secondary schools who use CISs.

  - ✓ This is achieved by training authorised CISs users on how to back-up vital information from their computers.
  - ✓ Trained CISs users should perform backups of critical information and should also be responsible for keeping the backup media safely for future use.

8.4.3. Physical controls guidelines

Although secondary schools enforced physical controls more than other controls, there were some deficiencies that needed to be addressed in order to improve security of CISs.

- ***Use of reliable physical controls***

Secondary schools should implement reliable physical controls that provide CISs assets adequate security and also making the environment where assets are used be safe for users. These include:

- ✓ Emphasis on physical security of all movable CISs hardware such as personal computers, hubs, cables
- ✓ Isolating computers used for CISs floor computer networks;
- ✓ Installing both fire and break-in alarms that will alert school security in the event of fire breakout or intruder being detected;
- ✓ Changing locking systems regularly in order to prevent duplication of keys by users;

The guidelines provided were not exhaustive, however, they played a crucial role in bolstering information security in secondary schools. These guidelines emphasised much on low cost security means that secondary schools could afford in most cases freely.

To conclude the discussions of this chapter, a summary of conclusions is given in section 8.5 below.

8.5. CONCLUSION

This section reflects on what transpired throughout this research study. Chapter 1 identified the need by secondary schools to protect their CISs. The study then proposed to help secondary schools perform risk management exercise for their CISs after noticing that these organisations relied a lot on computing facilities yet they did not have experts to deal with information security risks. Chapter 2 outlined the qualitative interpretive case study research methodology implemented in this research. Participatory observation was the main qualitative data collection technique aided by the interview and inspection techniques. Chapter 3 is an overview of information security and this is followed by discussions of risk management frameworks in Chapter 4. In Chapter 5, the researcher discussed quantitative and qualitative information security risk management methodologies and justified the use of OCTAVE-small for this research study. The OCTAVE-small method was discussed in detail in Chapter 6 and implemented in Chapter 7. Data were collected, presented, analysed and interpreted in Chapter 7. The findings of the study were stated and discussed based on respective objectives in Chapter 8 as research overview. The study went further to suggest generic risk protection and mitigation strategies that were commensurate with human and financial capabilities of secondary schools.

This study concluded that:

- Secondary schools, like any other small-scale organisations, have critical CISs assets that need to be secured;
- Secondary school managers were committed to information security to safeguard their CISs but lacked relevant skills and knowledge to achieve this;
- Secondary schools should continuously implement proper organisational security practice and technical controls to reduce security risks in their CISs;
- Educating and training of authorised users of CISs in information security plays crucial role in the security of CISs' critical asset in secondary schools; and
- The use of the OCTAVE-small method in risk management was effective in developing information security awareness among users of CISs who participated in this research.

These conclusions formed the basis on which recommendations to improve security controls in secondary schools were made. The subject of the next subsection is recommendations for security controls in secondary schools' CISs critical assets.

8.6. RECOMMENDATIONS FOR SECURITY CONTROLS

The study recommended that secondary schools put in place meaningful information security controls beyond those that were instituted during this study. This included the need for schools to continue carrying out regular risk management exercises for their CISs. The study also recommended that secondary schools:

- ✓ reduce the number of computers which were being used in computerising their information systems;
- ✓ disconnect all computers holding critical information from the Internet;
- ✓ supervise authorised users of CISs to reduce intentional information security breaches;
- ✓ make use of non-administrative educators who were competent in computing to administer all information technology assets and mentor the CISs users in various aspects of safe use of these assets;
- ✓ encourage all users of CISs to attend formal basic courses in computing and information security that will enrich them in computer operations and proper records management;
- ✓ use network passwords for each network segment for CISs and the passwords should only be known by responsible administrative educators;
- ✓ educate authorised users to use critical information systems assets responsibly and accountably by keeping their passwords confidentially;
- ✓ adhere to information security guidelines developed by the collaborative teams

Information security challenges that secondary schools have to overcome on daily basis have far reaching consequences on these organisations and this warrants further research in this area. The ultimate section of this chapter, Further Research is dedicated to this cause.

8.7. FURTHER RESEARCH

This case study successfully carried out information security risk management exercises in two secondary schools' CISs using a variant of the OCTAVE risk management strategy, streamlined for smaller organisations, namely the OCTAVE-small method. Due to the limitations of the original model, several alterations were made to the method so that it became suitable for use by CISs users who had baseline computing skills.

Due to the success of this research study, it is suggested that this study be expanded to study a larger representation of schools in this or other district(s), as well as to all levels of schools and other educational institutions. Alternatively, comparative studies of small-scale organisations, namely profit making and non-profit making could be carried out to identify suitable risk management models that are applicable to both categories of these organisations.

The most appropriate way to help secondary schools to overcome information security risks in their CISs could be developing risk management models which the personnel in these organisations will easily comprehend and be able to implement on their own. The model would be developed through full participation of secondary schools CISs users at all stages of its development cycle.

REFERENCES

Abdullah, H. 2006. *A risk analysis and risk management methodology for mitigating wireless local area networks WLANs intrusion security risks,* viewed 12 April 2011, from http://upetd.up.ac.za/thesis/submitted/etd-0122006155850/unrestricted/dissertation.pdf.

Al Saif, A. A. 2009. 'Risks associated with the use of the Internet and its impact upon students' awareness of pervasive issues', *Actica Didactia Napocensia- Literature review issues*. *2*(4) 200-250,

Alberts C. J., Behrens, S. G., Pethia, R. D. & Wilson, W. R. 1999. *Operationally Critical Threat, Asset, and Vulnerability Evaluations (OCTAVE*$^{(SM)}$*) Framework, Version 1.0.* Carnegie Mellon Software Engineering Institute, viewed 15 September 2012, from http://www.sei.cmu.edu/publications/pubweb.html.

Alberts, C. J. & Dorofee, A. 2001. *An introduction to OCTAVE SM Method*, viewed 15 September 2912, from http://www.cert.org/octave/methodintro.htm/#intro.

Alberts, C. J. & Dorofee, A. 2002. *Managing information security risks: The OCTAVE SM approach.* Boston: Addison-Wesley Anderson.

Alberts, C. J. & Dorofee, A. 2003. *Managing information security risks: the OCTAVE approach,*. Pearson Education, Inc. Boston

Alberts, C. J., Dorofee, A., Stevens, J. & Woody, C. 2003. *Introduction to the OCTAVE® Approach,* viewed 16 September 2012, from http://www.itgovernanceusa.com/files/Octave.pdf.

Alberts, C. J. & Dorofee A. 2004. *Using Vulnerability Assessment Tools to Develop an OCTAVE Risk Profile,* viewed 23 September 2004, from http://www.fish.com/satan/admin-guide-to-cracking.html.

Alhawari, S., Karadsheh, L., Talet, A. N. & Mansour, E. 2012. 'Knowledge-Based Risk Management framework for Information Technology Project', *International Journal of Information Management* 32(3) 50– 65

Anderson, E. E. & Choobineha, J. 2008. 'Enterprise information security strategies', *Computers & Security* 27(12), 22-29, viewed 10 September 2011, from http://www.elsevier.com.

AS/NZS ISO31000. 2009. *Australian - New Zealand Standard: Risk management - principles and guidelines*, viewed 21 June 2012, from http://sherq.org/31000.pdf.

Australian Capital Territory Insuarance Authority. 2004. *Guide to risk management,* viewed 15 October 2012, from http://www.treasury.actia.gov.au.actia/Guide.doc.

Aven, T. 2012. 'On the link between risk and exposure'. *Reliability Engineering and System Safety* 106(2) 191–199, viewed 29 July 2012, from http://www.elsevier.com/locate/ress.

Axelrod R. 2003. *Risk in Networked Information Systems,* viewed 15 March 2011, from http://www-personal.umich.edu/~axe/risk.pdf.

Babbie, E. 2007. *The practice of Social Research 11th Edition,* London, Thomson Learning Inc.

Babbie, E. R & Mouton, J. 2001. *The practice of social research*, Cape Town, Oxford University Press Southern Africa

Baino, P. 2001. 'Evaluations of security risks associated with networked information systems', Master of Business of Information Technology Thesis, Royal Melbourne Institute of Technology

Bauer, J. 2012. *What is a Firewall?,* viewed 22 June 2013, from http://portforward.com/help/firewalls.htm.

Beachboard, J. Cole, A., Mellor, M., Hernandez, S. & Aytes, K. 2008. 'Improving information security risk analysis practices for small and medium sized enterprises. A research Agenda', *Issues in Information Sciences and Technology 5*, 73-85.

Bednash, E. & Halstuch, J. 2010. *Data backup: Planning for failure*, viewed 21 July 2013, from http://www.racktopsystems.com/wp-content/uploads/2010/12/Racktop_WhitePaper_DataBackup-PlanningForFailure.pdf.

Bharadwaj, A. 2000. *Integrating Positivist and Interpretive Approaches to Information Systems Research: A Lakatosian Model*, viewed 13 April 2012, from http://www.bauer.uh.edu/parks/fis/Bharadwaj.htm.

Bozic, V. 2012. 'Risk Management in Information systems'. *Central European Conference on Information and Intelligent Systems* 337–345, September 2012, viewed 29 October 2012, from http://www.ceciis.foi.hr/app/public/conferences /1/papers2012/iss7.pdf.

Bozo, N. & Ruzic Dimitrijevic, L. 2009. 'Risk assessment of information technology systems', *Issues in Information Science and Information Technology,* 6, 2009, viewed 15 April 2011, from http://www.questia.com/library/journal/1G1-229896152/risk-assessment-of-information-technology-systems

Brass, P. 2011. *International Risk Management Standard AS/NZS ISO 31000:2009,* viewed 10 October 2012, from http://www.safa.sa.gov.au/documents/ins _ISO_31000.pps.

Broderick, J. S. 2001. 'Information security risk management – when should it be managed?' *Information Security Technical Report,* 6 (3) 12-18

Caballero, A. 2009. *Information Security Essentials for IT Managers: Protecting Mission-Critical Systems,* viewed 12 December 2012, from http://ebooks.narotama.ac.id/files/Managing%20Information%20Security/Chapter%201%20%20Information%20Security%20Essentials%20for%20IT%20Managers.pdf.

Campbell J. M. 2008. *Safety Hazard and Risk Identification and Management,* viewed 25 October 2013, from http://www.see.ed.ac.uk/IIE/research/ndtman/pubs/THESIS_JCampbell_May08.pdf.

Campbell, P, L. & Stamp, J. E. 2004. 'A Classification Scheme for Risk Assessment Methods', *SANDIA REPORT-SAND2004-4233. Sandia National Laboratories,* viewed 13 August 2012, from http://energy.sandia.gov/wp/wp-content/gallery/uploads /sand_2004_4233.pdf.

Canavan, J. E. 2001. *Fundamentals of Network Security,* Boston, viewed 12 April 2012, from http://www.artechhouse.com.

Cappelli, D. M. & Moore A. P. 2008. 'Risk Mitigation Strategies: Lessons Learned from Actual Insider Attacks', *CERT Program – Software Engineering Institute*, viewed 22 June 2012, from http://www.cert.org/archive/defcappellimoore0804.pdf.

Carothers, D. R. 2009. *Risk Identification Methods - From Checklists to Experts. Praxiom, v*iewed 20 October 2011, from http://praxiom.hubpages.com/hub/From-Checklists-to-Experts-The-Risk-Identificaton-Phase.

Cate, F. H. 2005. 'Information Security Breaches and the Threat to Consumers', *The Centre for Information Policy Leadership at Hunton & Williams LLP* September 2005, viewed 17 December 2012, from http://www.fredhcate.com/Publications/Information_Security_Breaches.pdf

Cavaye, A. L. M. 1996. 'Case study research: A multi-faceted research approach for IS'. *Information Systems Journal, 6(3)* 227–242, viewed 29 July 2013, from http://onlinelibrary.wiley.com/doi/10.1111/j.1365-2575.1996.tb00015.x/pdf

Chen, M. T. 2009. 'Information Security and Risk Management', *Encyclopaedia of Multimedia Technology and Networking, 2nd edition.* Idea Group Publishing, viewed 10 July 2012, from http://lyle.smu.edu/~tchen/papers/info-sec-risks.pdf.

Ciechanowicz, Z. 1997. 'Risk analysis: requirements, conflicts and problems*', Cornpurer and Srcuriq* 16. (3), 223-232, 1997. Elsevier Science Ltd.

Common vulnerabilities and exposures. 2012. *Terminology. The standard for information security vulnerability names,* viewed 27 April 2004, from http://cve.mitre.org/about/terminology.html.

Consultative, Objective and Bi-Functional Risk Analysis. 2005. 'Introduction to Security Risk Analysis', *Directory of information for security risk analysis and risk assessment,* viewed 28 October 2011, from http://www.security-risk-analysis.com/index.htm.

Cox, J. 2012. 'Information systems user security: A structured model of the knowing–doing gap', *Computers in Human Behaviour*, viewed 19 May 2013, from http://www.elsevier.com/locate/comphumbeh.

Cresswell, J. W. 2005. *Educational Research: Planning, conducting and evaluating quantitative and qualitative research,* 2nd Edition. New Jersey: Pearson Education Inc.

Creswell, J. W. & Miller, D. L. 2000. 'Determining validity in qualitative inquiry', *Theory into Practice, 39*(3), 124-131, viewed 15 May 2012, from DOI:10.1207/s15430421tip3903_2.

Crichton, D. 2009. *The Risk Triangle,* viewed 17 May 2011, from http://www.ilankelman.org/crichton/1999risktriangle.pdf.

Crowe C, Cresswell K, Robertson R, Huby G, Avery A, Sheikh A. 2011. *The case study approach. BMC Research Methodology, BMC Medical Research Methodology,* viewed 17 September 2012, from http://www.biomedcentral.com/1471-2288/11/100.

Darke, P., Shanks, G. & Broadbent, M. 1998. 'Successfully completing case study research: Combining rigour, relevance and pragmatism', Blackwell Science L.t.d. *Information Systems Journal 8 (4), 273–289,* viewed 12 May 2012, from http://www.uio.no/studier/emner/matnat/ifi/INF5500/h07/undervisningsmateriale/ISJ_case_study.pdf.

de Villers M. R. 2005. *Interpretive research models for informatics: action research, grounded theory and the family of design and development research, viewed from* 12 May 2012, from http://alternation.ukzn.ac.za/docs/12.2/02%20deV.pdf.

Denzin, N. K. & Lincolin, Y. 2008. *Collecting and interpreting qualitative material,.* Califonia: SAGE Publications.

Department of Environmental Affairs and Tourism, 2006. 'Risk Management', *Integrated Environmental Management Information Series 23,* viewed 21 February 2012, from http://www.deat.gov.za.

De Vaus, D. A. *Research Design in Social Research*. London: SAGE, 2001. http://libguides.usc.edu/content.php?pid=83009&sid=818072

Dimopoulos, V., Furnell, S. & Barlow, I. 2003. *Considering IT Risk analysis in small and medium enterprises*, viewed 10 September 2011, from http://scissce.scis.educ.au/proceedings/2003/inforsec/pdf/02_final.pdf.

Ding, T. 2002. *Quantitative Risk Analysis Step-by-step. A Practical Version*, SANS reading room, viewed 20 May 2012, from http://www.sans.org/reading_room/whitepapers/auditing/quantitative-risk-analysis-step-by-step_849.

Doherty, N. F & Fulford, H. 2006. 'Aligning the information security policy with the strategic information systems plan', Elsevier, *Computers and Security* 25, 55–63, viewed 29 March 2013, from http://www.sciencedirect.com

Dooley, L. M. 2002. 'Case Study Research and Theory Building.' *Advances in Developing Human Resources* 4(3) August 2002. Sage Publications

Dorian, L. 2012. *Risk Management: Understanding Industry Insights*, viewed 28 August 2013, from http://www.ica.bc.ca/ii/ii.php?catid=17.

Edwards, R. 2010. *How to do Risk Assessment*, viewed 15 March 2013, from http://riskcommentary.com/how-to-do-risk-assessment-e93-first-establish-the-context.

Elky, S. 2006. *An Introduction to Information System Risk Management,* SANS Institute InfoSec Reading Room SANS Institute, viewed 16 April 2011, from http://www.sans.org/reading_room/whitepapers/auditing/introduction-information-system-risk-management_1204.

Elyse, S. 2007. *Risk Identification*, viewed 21 May 2011, from http://www.anticlue.net/archives/000816.htm.

Evaluation Briefs, 2008. *Data Collection Methods for Program Evaluation*, Observation, No. 16, December 2008, viewed 16 April 2012, from http://www.cdc.gov/healthyyouth/evaluation/pdf/brief16.pdf

Falconer, D. J. & Mackay, D. R. 1999. 'The Key to the Mixed Method Dilemma' In: *Proceedings of 10th Australasian Conference on Information Systems, 1999*, viewed 15 October 2011, from http://citeseerx.ist.psu.edu/viewdoc/download?doi:10.1.1.5.148&rep=rep1&type_pdf

Federal Highway Administration. 2007. *Risk Assessment and Allocation for Highway Construction Management,* viewed 15 October 2012, from http://international.fhwa.dot.gov/riskassess/index.cfm.

Feng, N. & Li, M. 2011. 'An information systems security risk assessment model under uncertain environment', *Applied Soft Computing 11(7), 4332–4340, October 2011,* viewed 15 October 2012, from http://www.sciencedirect.com/science/journal.

Foster, P. 2006. 'Observational Research: Data Collection', *Qualitative Research,* 57-59. London, SAGE Publications L.t.d.

Ganthan, N. S., Rabiah, A. & Zuraini I. 2009. 'Adopting and Adapting Medical Approach in Risk Management Process for Analysing Information Security Risk', *Risk Management for the Future – Theory and Cases,* 368–388, viewed 17 May 2012, from http://cdn.intechopen.com/pdfs/36111/InTech-adopting_and_adapting_medical_approach_in_risk_management_process_for_analysing_information_security_risk.pdf

GAO/AIMD-00-33. 1999. Information security risk assessment practices of leading organisations, *A Supplement to General Accounting Office (GAO)'s May 1998 Executive Guide on Information Security Management,* viewed 18 December 2011, from http://www.gao.gov/products/AIMD-00-33.

Gerber, A. J. 2006. *Towards a comprehensive functional layered architecture for the semantic web,* PhD Thesis in Computer Science. University of South Africa (UNISA), viewed 21 May 2012, from http://uir.unisa.ac.za/bitstream/handle/10500/1494/thesis.pdf?sequence=1

Gerber, M. & von Solms, R. 2001. 'From risk analysis to security Requirements', *Computer and Security* 20(7), 31 October 2001, 577-584.

Galea Francheschini Innovation White Paper, 2005. *Patch management: Fixing vulnerabilities before they are exploited*, viewed 20 September 2013, from http://www.gfi.com/whitepapers/fixingvulnerabilitiesbeforetheyareexploited_EN_GEN_wp.pdf.

Goel, S. & Chen, V. 2008. 'Can business process reengineering lead to security vulnerabilities: Analysing the reengineered process', *Production Economics 115 104–112*.

Golafshani, N. 2003. 'Understanding Reliability and Validity in Qualitative Research', *The Qualitative Report* 8(4), 597-607, December 2003, viewed 13 January 2013, from http://www.nova.edu/ssss/QR/QR8-4/golafshani.pdf.

Goldkuhl, G. 2012. 'Pragmatism versus interpretivism in qualitative information systems research', *European Journal of Information Systems*, 21(2), 135-146.viewed 13 May 2012, from http://dx.doi.org/10.1057/ejis.2011.54

Goldkuhl, G. 2008. What kind of pragmatism is in information Systems research?, *AIS SIG Prag Inaugural meeting,* Dec 14, 2008, Paris, viewed 13 May 2013, from http://www.vits.org/publikationer/dokument/663.pdf.

Gray, D. E. 2009. *Doing research in the real world.* London, SAGE Publication L.t.d.

Guidance Consulting Inc. 2012. *Data Recovery - the importance of data backups*, viewed 15 July 2013, from http://www.guidance-consulting.com/articles/60-importance-of-data-backups-.html.

Gundlach, M. 2011. *Risk Mitigation Strategies and Risk Mitigation Plan*, viewed 19 August 2013, from http://www.brighthub.com/office/project-management/articles/47934.aspx.

Hancock, B. 2002. *An Introduction to Qualitative Research. Trent Focus Group,* viewed 12 March 2009, from http://www.libreriafarmaceutica.com/cover_note/books/4/8/5/9780387245584/9780387245584-c1.pdf.

Hansche S. 2001. 'Designing a security awareness program: Part I', *Information System Security* 10(1), 14–22.

Harper, E. 2002. *OCTAVE Developers reach out to Smaller Organisations with OCTAVE-*small, viewed 15 May 2013, from http://www.sei.cmu.edu/library/abstracts/news-at-sei/ feature14q02.cfm

Hoo, K. J. S. 2000. *How much security is enough? A risk-Management approach to computer security - A working paper*, Consortium for research on Information security and Policy, viewed 20 April 2011, from http://wwww.cisac.stanford.edu/ publications/how_much_is_enough__a_risk_management_approach_to_computer_ security.pdf.

Jenkins, B. D. 1998. *Security Risk analysis and amangement*, viewed 18 August 2011, from http://www.nr.no/~abie/RA_by_Jenkins.pdf.

Jones, A & Ashenden, D. 2005. *Risk management for computer security: Protection of your network and information asset,*. Lincare House, Jordan Hill, Oxford.

Karabacaka, B. & Sogukpinar, I. 2003. 'ISRAM: information security risk analysis method.' *Computers and Security* 24(2), 147 -159.

Karyda, M., Kiountouzis, E. & Kokolakis, S. 2004. 'Information systems security policies: a contextual perspective', *Computers & Security* 24(2), 246-260. Elsevier Ltd

Kassner, M. 2009. *Ten ways to avoid IT security breaches*, viewed 12 October 2011, from http://hosteddocs.ittoolbox.com/KC032505.pdf.

Katsikasa, S. K. 2009. 'Risk Management in Computer and Information Security', *Hand Book.* Morgan Kaufmann, Inc.,605-625

Kim, S. 2003. 'Research Paradigms in Organisational Learning and Performance: Competing Modes of Inquiry', *Information Technology, Learning, and Performance Journal 21(1), Spring 2003*, viewed 17 April 2012, from http://www.osra.org/itlpj/kimspring2003.pdf.

Kirupakar. B. R .2007. 'Quality Risk Management for Pharmaceutical Industry', *Pharmaceutical Reviews* 5(1) January 2007, viewed 20 September 2011, from http://www.pharmainfo.net/latest-reviews.

Kite, M. J. S. 2009. *Information Security Policy*, viewed 17 May 2013, from http://www.abdn.ac.uk/hr/uploads/files/information-security-policy.pdf.

Krauss, S. E. 2005. 'Research Paradigms and Meaning Making: A Primer', *The Qualitative Report* 10(4) December 2005 758-770, viewed 20 May 2012, from http://www.nova.edu/ssss/QR/QR10-4/krauss.pdf.

Lander, V. 2004, Choosing a risk assessment mwthodology. *BioPharm International,* viewed 17 October 2012, from http://www.taika.com/files/21-cfr-part11-choosing-a-risk-asseesment-methodology.pdf.

Leech, N. L. & Onwuegbusie, A. 2007. 'An array of qualitative data analysis tools: A call for data analysis triangulation', *School of Psychology/Quarterly* 22(4), 557-584.

Lincoln, Y. S. & Gobi, E. G. 1985. *Naturalistic Inquiry,* Newbury Park, CA: Sage Publications

Lo, C. C. & Chen, W. J. 2012. 'A hybrid information security risk assessment procedure considering interdependences between controls', *Expert Systems with Applications* 39 (2012) 247–257, viewed 27 February 2013, from http://www.rmcet.com/lib/E-Journals/Expert%20Systems%20with%20Applications/Volume%2039,%20Issue%201,20Pages%201594%20(January%202012)/A%20hybrid%20information%20security%20risk%20assessment%20procedure%20considering.pdf

Mah, P. 2012. *Three Reasons for Proper Data Backup Matter*, viewed 12 October 2012, from http://www.smallbusinesscomputing.com/news/3-reasons-proper-data-backup-matters.html.

Marchany, R. 2003. *Conducting risk analysis: Computer Network in Higher Education.* Educause, viewed 20 September 2011, from http://net.educause.edu/ir/library/pdf/pub7008g.pdf.

Mark, N., Woodsong, C. K., Guest, G, & Namey, E. 2005. Qualitative Research Methods: A Data Collector's Field Guide', *Family Health International*, viewed 20 May 2012, from http://pdf.usaid.gov/pdf_docs/PNADK310.pdf.

Marshall, C. & Rossmann, G. B. 2006. *Designing Qualitative Research 4th edition*, Thousand Oaks: SAGE Publications, London.

Maxwell, J. A. 2008. *Designing a Qualitative Study*, viewed 25 July 2013, from http://coursesite.uhcl.edu/HSH/PeresSc/Classes/PSYC6036www/presentations/Ch7_qualitativeResearch.pdf.

Mazareanu, V. 2007. *Risk Management and Analysis: Risk Assessment Qualitative and Quantitative, viewed 20 April 2011, from* http://papers.ssrn.com/sol13/papers.cfm?abstractid=1549186.

McGraw, E. 2005. *Risk Management Framework (RMF).* Digital, Inc., viewed 20 April 2011, from https://buildsecurityin.us-cert.gov/bsi/articles/best-practices/risk/250-BSI.html.

Meek, D.S. 2005. *Risk Analysis Framework,* viewed 20 May 2011, from http://www.ogtr.gov.au/internet/ogtr/publishing.nsf/content/raf3/$FILE/raffinal2.2.pdf

Meier, J.D. Mackman, A., Dunner, M., Vasireddy, S., Escamilla, R & Murukan, A. 2006. *Improving Web Application Security: Threats and Controls*, viewed 23 September 2011, from http://msdn.microsoft.com/en-us/library/ff648641.aspx.

Merriam, S. B. 2009. *Qualitative research: A guide to design and implementation*, San Francisco: Jossey Boss. Wiley Imprints.

Metras, R. 2008. Risk Analysis and Risk Assessment. Ibadan, 15-17th Oct 2008

Microsoft help and support. 2013. *How to Remove Win32 Trojan*, viewed 29 October 2013, from http://speedmaxpc.com/lp/spyware/?t202id=4122&t202kw=win32Trojan&n=001 &gclid=CNvd4-GymboCFY_KtAodCk4Acw.

Microsoft TechNet. 2006. *Strategies for Managing Malware Risks*, 24 July 2013, from http://technet.microsoft.com/en-us/library/cc875806.aspx.

Miles, M. B. & Huberman, A. M. 1994. *Qualitative Data Analysis,* SAGE Publications, Thousands Oarks, London.

Morse, J. M., Barrett, M., Mayan, M., Olson, K. & Spiers, J. 2002. 'Verification Strategies for Establishing Reliability and Validity in Qualitative Research', *International Journal of Qualitative Methods* 1(2), Spring 2002, viewed 21 September 2011, from http://www.ualberta.ca/~ijqm/.

Mouton, J. 2009. *Understanding social research,* Van Schaik Publishers, Pretoria

Mraz, M. & Huber, B. 2005. *FMEA – FMECA*, viewed 12 March 2011, from http://www.fmeainforcenter.com/updates/huber2005 FMEA.pdf+FMEA/FMECA.

Mutchnick, R. J. & Berg, B. L. 1996. *Research methods for social sciences: Practical and applications*, Allyn and Bacon, Boston.

Myers, M. D. 2004. *Qualitative research in information systems,* viewed 15 September 2011, from http://www.staff.business.auckland.ac.nz/mMyers.

Myers, M. D. 2009. *Qualitative Research in Business & Management*, Sage Publications, London.

Myers, M. D. 2011. 'Qualitative Research in Information Systems', *MIS Quarterly* 21(2), 241-242, 17 February 2011, viewed 29 June 2012, from http://www.misq.org/discovery/MISQD_isworld.

Myers, M. D. and Avison, D.E. (eds) 2002. *Qualitative Research in Information System,*. Sage Publications, London.

National Treasury Republic of South Africa. 2007. *Framework for managing programme performance information*, Formeset Printers Cape (Pty) Ltd. May 2007, viewed 20 April 2012, from http://www.treasury.gov.za/publications/guidelines/FMPI.pdf.

Navarro, L. 2001. 'Information Security Risks and Managed Security Service', *Information Security Technical Report* 6(3) 28-36

Nienaber, R. C. 2008. *A model for enhancing software project management using software agents*, PhD Thesis University of South Africa (UNISA), viewed 10 April 2012, from http://uir.unisa.ac.za/bitstream/handle/10500/2296/thesis.pdf?sequence=1

Noor, K. B. 2008. 'Case study: A strategic Research Methodology', *American Journal of Applied sciences* 5(11), 1602 - 1604.

Nosworthy, J. D. 2000. 'A Practical risk analysis approach: Managing risks', *Computers & Security*, 19 (2000) 596-614

Nyame-Asiamah, F & Patel, N. 2009. Research methods and methodologies for studying organisational learning, *European and Mediterranean Conference on Information Systems* 13-14 July *2009*, Crowne Plaza Hotel, Izmir

Oates, B. 2006. *Researching Information Systems and Computing*, London: Sage Publications Ltd.

O'Donnell, G. & Best, B. 2005. *Conducting school risk assessment, risk management and managing resources,* Optimums Professional Publishing Limited, viewed 13 April 2012, from http://www.teachingexpertise.com/articles/conducting-school-risk-assessment-risk-management-and-managing-resources-1299.

Panda, P. 2009. 'The OCTAVE-R approach to information security risk assessmenmt'. *Journal of Past Issues* 4(3) 17-29, viewed 20 May 2011, from http://www.isaca.org.Journal/past-issues/2009/volume4/documents/jpdf09-OCTAVE.pdf.

Pare, G., Sicotte, C., Jaana, M., & Girouard, M.S. D. 2008. Prioritizing Clinical Information System Project Risk Factors: A Delphi Study proceedings of the 41st Hawaii International Conference on System Sciences, viewed 12 March 2012, from www.ncbi.nlm.nih.gov/pubmed/18473092

Park, S. T., Min, B., Lee, I., Lee, G. & Lee, J. 2006. Evaluation Mthod for information security Levels of CIIP Critical information infrastructure Protection, *World Academy of science Enginnering and Technology*.

Potter, C. & Beard, A. 2010. *Information Security Breaches Survey.* technical report 2010, viewed 17 November 2012, from www.infosec.co.uk.

Pilici, S. 2013. *Remove TrojanDownloader:Win32/Adload.DA* (Removal Guide), viewed 20 November 2013, form http://malwaretips.com/blogs/trojandownloader-win32-adload-da-virus/

Potter, C. & Waterfall, G. 2012. *Information security breaches survey technical report,* viewed 27 August 2013, from http://www.pwc.co.uk/en_UK/uk/assets /pdf/olpapp/uk-information-security-breaches-survey-technical-report.pdf.

Putvinski, M. 12012. *Information technology security series*, Information security best practices viewed 30 August 2013, from http://www.corporatecomplianceinsights.com/author/matthew-putvinski.

Pyka, M. & Januszkiewicz, P. 2006. 'The OCTAVE$^{(SM)}$ methodology as a risk analysis tool for business resources', *Computer Science and Information Technology*. 485-497.

Rainer, R. K., Snyder, C. A., & Carr, H. H. 1991. 'Risk analysis for information technology', *Journal of Management Information Systems.* 8(1), 129-147.

Rausand, M. 2005. HAZOP: *Hazard and operability Study. System Reliability Theory,* viewed 31 October 2011, from http://www.ntnu.no/ross.slides/hazop.pdf+HAZOP.

Renfroe, N. A. and Smith, J. L. 2011. *Threat/Vulnerability Assessments and Risk Analysis,* Applied Research Associates Inc, viewed 20 April 2013, from http://www.wbdg.org /resources/riskanalysis.php#top

Rezgui, Y & Marks, A. 2008. 'Information security awareness in higher education: An exploratory study', *Computers & Security* 27(7), 241-253, viewed 15 April 2013, from http://www.emeraldinsight.com/bibliographic_databases.htm?id=1766195:DOI:10.1016/j.cose.2008.07.008

Richard, A., Caralli, R. A., Stevens, J. F., Young, L. R. & Wilson, R. W. 2007. *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process.* Software Engineering Institute. Carnegie Mellon University, viewed 13 November 2012, from http://www.cert.org/archive/pdf/07tr012.pdf.

Ritchie, J. & Lewis, J. 2005. *Qualitative research practice: A guide for Social Science Students and Researcher,.* London: SAGE Publications.

Rot, A. 2008. 'IT Risk Assessment: Quantitative and Qualitative Approach', *World Congress on Engineering and Computer Science WCECS*. 22-24 October 2008, San Francisco: SANS.

Rouse, M. 2007. *Firewall,* viewed 17 August 2013, from http://searchsecurity.techtarget.com/definition/firewall

Sarkar, K. R. 2010. 'Assessing insider threats to information security using technical, behavioural and organisational measures', *Information Security Technical Report* 15, 112-133, views 15 February 2012, from www.compseconline.com/publications/prodinf.htm

Schmidt, D. 2011. *Data Breaches: A Year in Review,* Clearinghouse, viewed 21 August 2011, from https://www.privacyrights.org/top-data-breach-list-2011

Shanks, G and Parr, A. 2003. 'Positivist, Single Case Study Research in Information Systems: A Critical Analysis'. In: *Proceedings of the 11th European Conference on Information Systems,* ECIS 2003, Naples, Italy 16-21 June 2003, viewed 23 October 2012, from http://www.researchgate.net/publication/221409527_Positivist_single_case_study_research_in_information_systems_a_critical_analysis.

Shortreed, J. 2008. *ISO 31000 – Risk Management Standard,* viewed 20 June 2012, from http://www.irr-neram.ca/pdf_files/ISO%2031000.pdf

Shortreed, J., Hicks, J & Craig, L. 2003. *Basic Frameworks for Risk Management,* Final Report March 28, 2003 Prepared for The Ontario Ministry of the Environment, viewed 12 April 2012, from http://www.irrneram.ca/pdf_files/basicFrameworkMar2003.pdf.

Siu, T. 2007. *Information Scecurity Risk management,* viewed 13 September 2012, from http://wiki.edu/information_security_risk_kanagement:Overarching_themes.

Sosonkin, M. 2005. OCTAVE: Operationally Critical Threat, Asset and Vulnerability Evaluation, viewed 20 June 2011, from http://isis.poly.edu/courses/cs996-management-s2005/Lectures/octave.pdf.

South African Centre for Information Security. 2010. *Welcome to South African Centre for Information Security,* viewed 10 November 2013, from http://sacfis.co.za/.

Steele, S., & Wargo, C. 2007. 'An introduction to insider threat management', *Information Systems Security,* 16(1) 23–34, viewed 20 September 2011, from http://www.infolocktech.com/download/ITM_Whitepaper.pdf

Steve, E. 2007. *An Introduction to information systems risk management,* Sans Institute Reading Room, viewed 18 September 2011 from http://www.sans.org/reading_room.

Stevens, J. 2005. 'Information Asset Profiling', *(CMU/SEI-2005-TN-021, ADA441305). Pittsburgh, PA: Software Engineering Institute,* Carnegie Mellon University, viewed 23 March 2012, from http://www.sei.cmu.edu/publications/documents/05.reports/05tn021.html

Stockdale, R. & Standing, C. 2006. *An interpretive approach to evaluating information systems: A content, context, process framework,* viewed 10 October 2011, from www.elsevier.com/locate/ejor.

Stoneburner, G., Goguen, A. & Feringa, A. 2002. Risk management Guide for Information Technology Systems. *NIST Special Publication* 800-30, viewed 24 September 2011 from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

Storms, A. 2003. *Using vulnerability assessment tools to develop an OCTAVE risk profile,* viewed 12 May 2012, from http://www.sans.org/reading_room.

Sveen, F. O, Torres, J. M. and Sarriegi, M. J. 2009. 'Blind information security strategy', *International Journal of Critical Infrastructure Protection,* 2(4) 95-109

Taylor, A., Alexander, D., Finch, A & Sutton, D. 2008. Information Security Management Principles: An ISEB Certificate. *The British Computer Society',* Publishing and Information Products, Swindon, viewed 15 November 2012, from http://www.bcs.org.

Taylor, B and Azadegan, S. 2007. Using Security Checklists and Scorecards in CS Curriculum. In: '*Proceedings of the 11th Colloquium for Information Systems Security,* Education Boston, MA June 4-7, 2007, viewed 08 September 2011, from https:/citeseerx.ist.psu.edu/using-security-checklists-and-score-cards-in-cs-curriculum.pdf.

Tere, R. 2006. *Qualitative data analysis,* viewed 13 September 2012, from http://e-articles.info/e/s/s/Science-and-research/QUALITATIVE-DATA-ANALYSIS.htm.

TerreBlanche, M. and Durrheim, K. 1999. *Research in Practice Applied methods for the social sciences,* Cape Town: University of Cape Town Press

The Association of Insurance and Risk Managers (AIRMIC), the National Forum for Risk Management (ALARM) and the Institute of Risk Management (IRM). 2002. *A Risk Management Standard*, viewed 14 April 2012, http://www.theirm.org/ publications/ documents/Risk_Management_Standard_030820.pdf.

The State of Queensland (Queensland Treasury). 2011. *A Guide to Risk Management,* viewed 19 August 2012, from http://www.treasury.qld.gov.au/office/knowledge/docs/risk-management-guide/guide-to-risk-management.pdf.

Theoharidou, M., Kokolakis, S., Karyda, M. & Kiountouzis, E. 2005. 'The insider threat to information systems and the effectiveness of ISO17799', *Computers and Security 24(6),* 472-484, September 2005, viewed 16 July 2011, from www.elsevier.com/locate/cose.

Thiagarajan, V. B.E. 2003. *Information Security Management*, viewed 14 June 2011, from http://www.best-management-practice.com/gempdf/itilv3_and_information_ security09.pdf.

Tiwari, A. 2010. *Information Security Risk Management: An Overview Risk Management*: *An Essential Guide to Protecting Critical Assets,* viewed 19 September 2012, from http://www.suite101.com/profile.cfm.

Tohidi, H. 2010. 'The Role of Risk Management in IT systems of organisations', In: World Conference on Information Technology *Procedia Computer Science* 3, 881–887, viewed 01 February 2013, from http://ac.els-cdn.com/ S1877050910005193/1-s2.0-S1877050910005193-main.pdf?_tid=0408e64a-7c75-11e3-ab50-00000aab0f26&acdnat=1389632957_ ffe4541faa5e24593e2aad24a624b5be

Toolsjournal. 2010. *Risk Identification Techniques,* viewed 15 July 2011, from http://www.toolsjournal. com/management-methodologies/itemlist/user/80-toolsjournal.

Trochim, W. M. K. 2006. *Qualitative Validity,* viewed 05 October 2012, from http://www.socialresearchmethods.net/kb/qualval.php.

United States Department of Commerce Office of Security, 2011. Analytical Risk Management: A Systems Approach to Security Decision Making

United States of America Department of Home Security (DHS). 2010. *DHS Risk Lexicon Edition*, viewed 19 September 2011, from http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf.

van Niekerk, L. 2005. *Information Security Risk Management in the South African Small, Medium and Micro Enterprise Environment: The Peculium Model*: Dissertation Submitted for Master of Science in Informatics at the University of Johannesburg, viewed 12 October 11, from https://ujdigispace.uj.ac.za/bitstream/ handle/10210/761/DissertationLVN_27June.pdf? sequence=1

Violino, B. 2010. *IT risk assessment frameworks: real-world experience*, viewed 27 June 2011, from http://www.csoonline.com/article/592525/it-risk-assessment-frameworks-real-world-experience

Voss, C., Tsikriktsis, N. & Frohlich, M. 2002. 'Case research operations Management', *International Journal of Operations & Production Management* 22 (2), 2002, 195-219, viewed 19 May 2012, from http://www.emeraldinsight.com/0144-3577.

Wack, J., Tracy, M., & Souppaya, M. 2003, 'Guidelines on Network Security Testing and Computer Security', *NIST Special publication* 800, 30-42, October 2003.

Walsh, T. 2011. *Health Information Security Risk Analysis Handbook for Kansas Hospitals and Health Care Providers,* viewed 17 April 2011, from www.kha-net.org/furtherinformation/downloadshitcriticalissues/d86746.aspx+how+to+process+data+from+octave+worksheets&cd=34&hl=en&ct=clnk&gl=za.

Walsham. G. 2006. 'Doing Interpretive Research', *European Journal of Information Systems*, 15(3) 320-330, viewed http://www.citeulike.org/user/Mandre/article/4540077.

Warden, B & Wong, S. 2007. *Introduction to qualitative analysis*, New York: Constella Group.

Wawrzyniak, D. 2006. *Information Security Risk Assessment Model for Risk Management,* viewed 29 March 2012, from http://link.springer.com/chapter/10.1007%2F11824633_3#page-2.

Weber, R. 2004. The Rhetoric of Positivism versus Interpretivism, *MIS Quarterly* 28 (1) 56-68

Werlinger, R., Hawkey, K., Botta, D., & Beznosov, K. 2009. 'Security practioners in context: Their activities and interactions with other stakeholders within organisations', *International Journal Human-Computer Studies. 67* (5), 584-606.

Williams P. A. H. 2008. ‘In a trusting environment, everyone is responsible for information’, *Security Information Security Technical Report 13.* 207–21, viewed 26 February 2012, from www.compseconline.com/publications/prodinf.htm.

Wold, G. H. & Shriver, R. F. 1997. ‘Risk analysis techniques: The risk analysis process provides the foundation for the entire recovery planning effort’, *Disaster Recovery World and Disaster Recovery Journal* 7(3), viewed 12 April 2011, from http://www.drj.com/new2dr/newbies.htm.

Woody, C., Coleman, J., Fancher, M., Myers, C. & Young, L. 2006. *Applying OCTAVE*: *Practitioners Report,* viewed 24 May 2012, from http://www.sei.cmu.edu/publications/pubweb.html/06tn010.pdf.

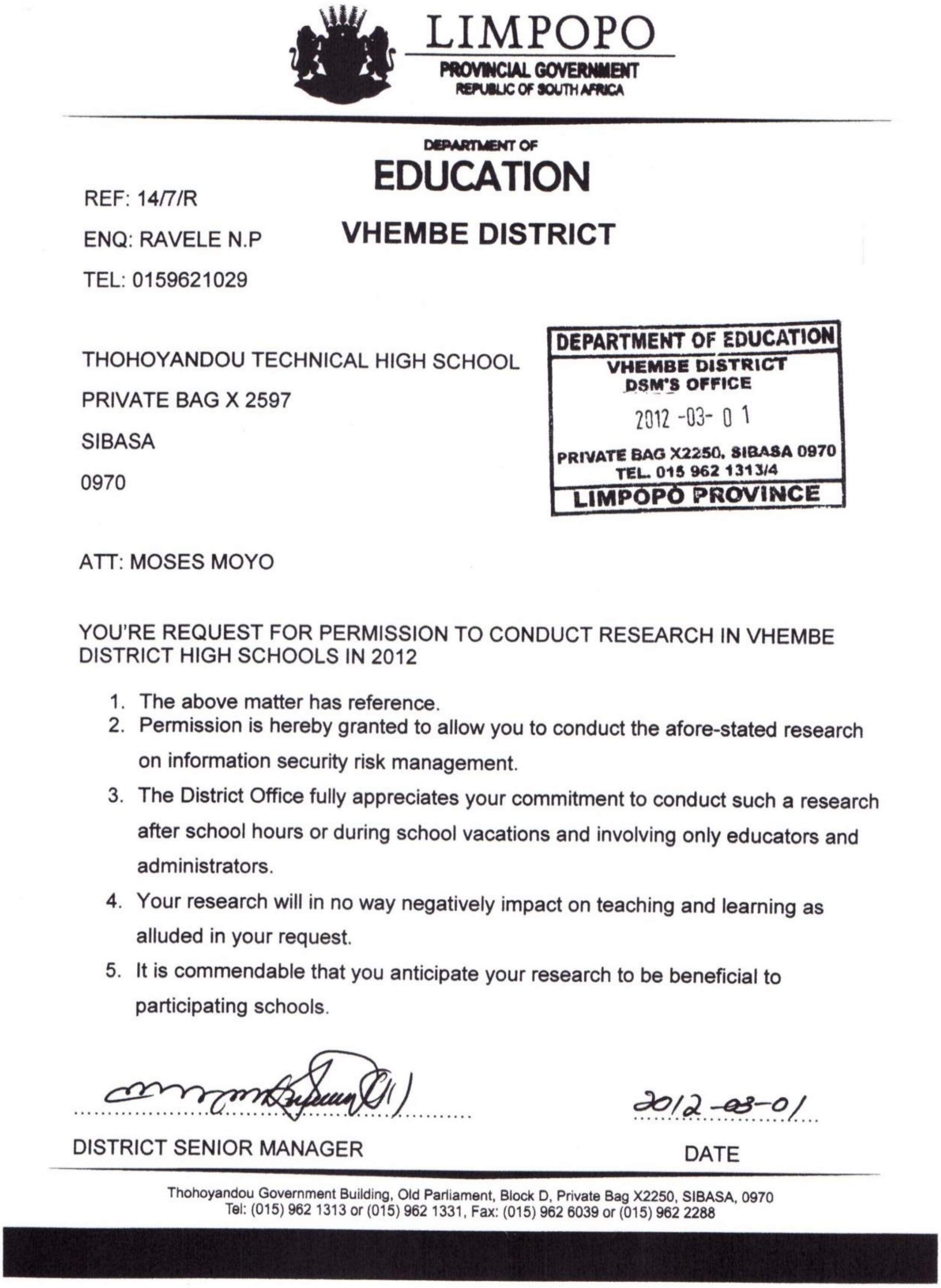
Yazar, Z. 2004. *A qualitative risk analysis and management tool – CRAMM*, viewed 14 October 2011, from http://www.sans.org/reading-room/whitepapers/auditing/qualitative-risk-analysis-management-tool-cramm-83?show=qualitative-risk-analysis-management-tool-cramm-83&catauditing.

Yeha, Q. J. & Chang, A. 2007. ‘Threats and controls for information system security. A cross-industry study’, *Information management* 44(5), July 2007, 480 - 49

Yin, R. K. 2003. *Case study research: Design and methods* 3rd, Thousand Oaks, Sage, California

APPENDICES

APPENDIX 1: DEPARTMENT OF EDUCATION LETTER OF APPROVAL



LIMPOPO
PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF
EDUCATION
VHEMBE DISTRICT

REF: 14/7/R
ENQ: RAVELE N.P
TEL: 0159621029

DEPARTMENT OF EDUCATION
VHEMBE DISTRICT
DSM'S OFFICE
2012 -03- 0 1
PRIVATE BAG X2250, SIBASA 0970
TEL. 015 962 1313/4
LIMPOPO PROVINCE

THOHOYANDOU TECHNICAL HIGH SCHOOL
PRIVATE BAG X 2597
SIBASA
0970

ATT: MOSES MOYO

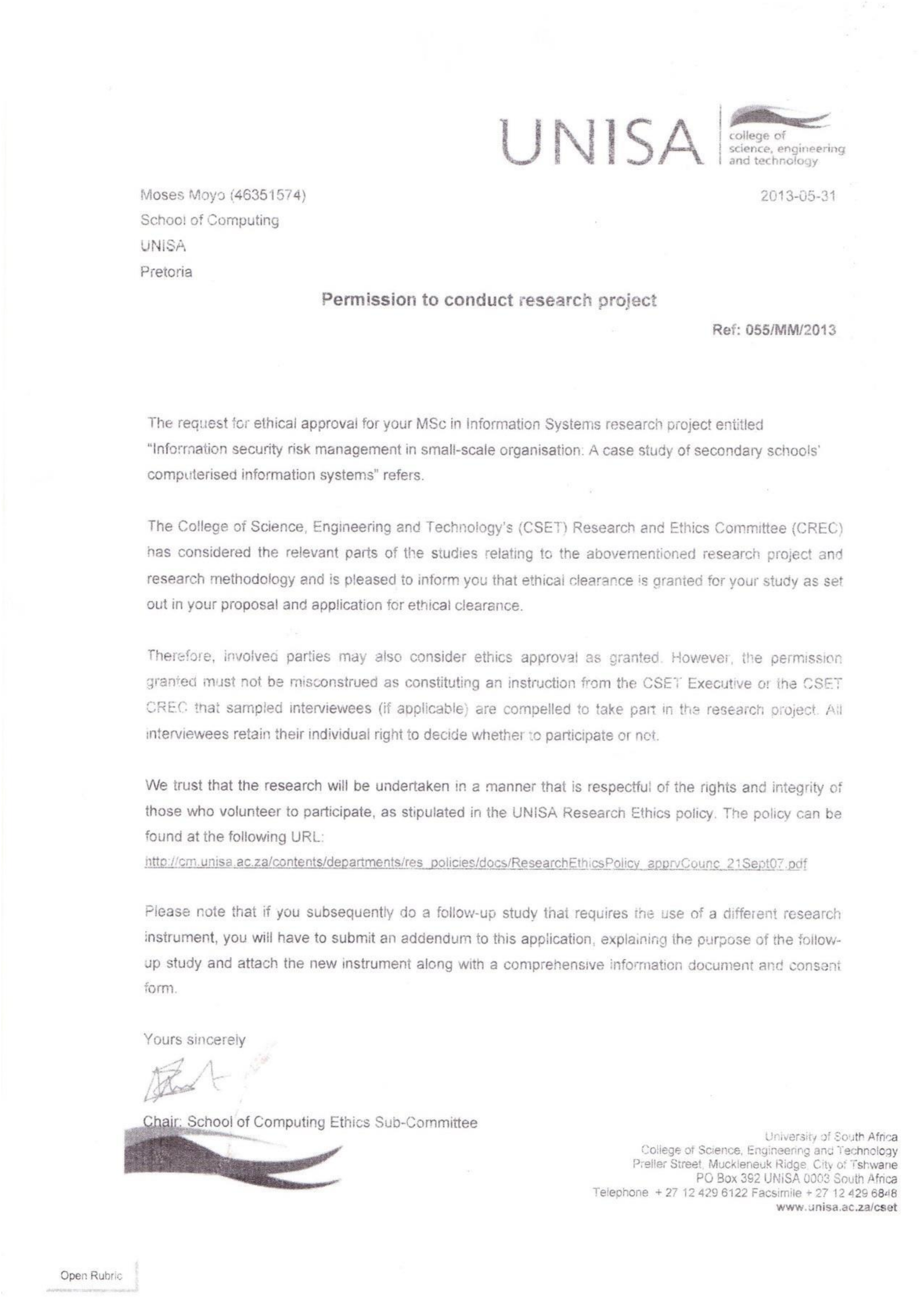
YOU'RE REQUEST FOR PERMISSION TO CONDUCT RESEARCH IN VHEMBE DISTRICT HIGH SCHOOLS IN 2012

1. The above matter has reference.
2. Permission is hereby granted to allow you to conduct the afore-stated research on information security risk management.
3. The District Office fully appreciates your commitment to conduct such a research after school hours or during school vacations and involving only educators and administrators.
4. Your research will in no way negatively impact on teaching and learning as alluded in your request.
5. It is commendable that you anticipate your research to be beneficial to participating schools.

.... 2012-03-01
DISTRICT SENIOR MANAGER DATE

Thohoyandou Government Building, Old Parliament, Block D, Private Bag X2250, SIBASA, 0970
Tel: (015) 962 1313 or (015) 962 1331, Fax: (015) 962 6039 or (015) 962 2288

APPENDIX 2: ETHICAL CLEARANCE LETTER FROM UNISA



UNISA college of science, engineering and technology

Moses Moyo (46351574)
School of Computing
UNISA
Pretoria

2013-05-31

Permission to conduct research project

Ref: 055/MM/2013

The request for ethical approval for your MSc in Information Systems research project entitled "Information security risk management in small-scale organisation: A case study of secondary schools' computerised information systems" refers.

The College of Science, Engineering and Technology's (CSET) Research and Ethics Committee (CREC) has considered the relevant parts of the studies relating to the abovementioned research project and research methodology and is pleased to inform you that ethical clearance is granted for your study as set out in your proposal and application for ethical clearance.

Therefore, involved parties may also consider ethics approval as granted. However, the permission granted must not be misconstrued as constituting an instruction from the CSET Executive or the CSET CREC that sampled interviewees (if applicable) are compelled to take part in the research project. All interviewees retain their individual right to decide whether to participate or not.

We trust that the research will be undertaken in a manner that is respectful of the rights and integrity of those who volunteer to participate, as stipulated in the UNISA Research Ethics policy. The policy can be found at the following URL:
http://cm.unisa.ac.za/contents/departments/res_policies/docs/ResearchEthicsPolicy_apprvCounc_21Sept07.pdf

Please note that if you subsequently do a follow-up study that requires the use of a different research instrument, you will have to submit an addendum to this application, explaining the purpose of the follow-up study and attach the new instrument along with a comprehensive information document and consent form.

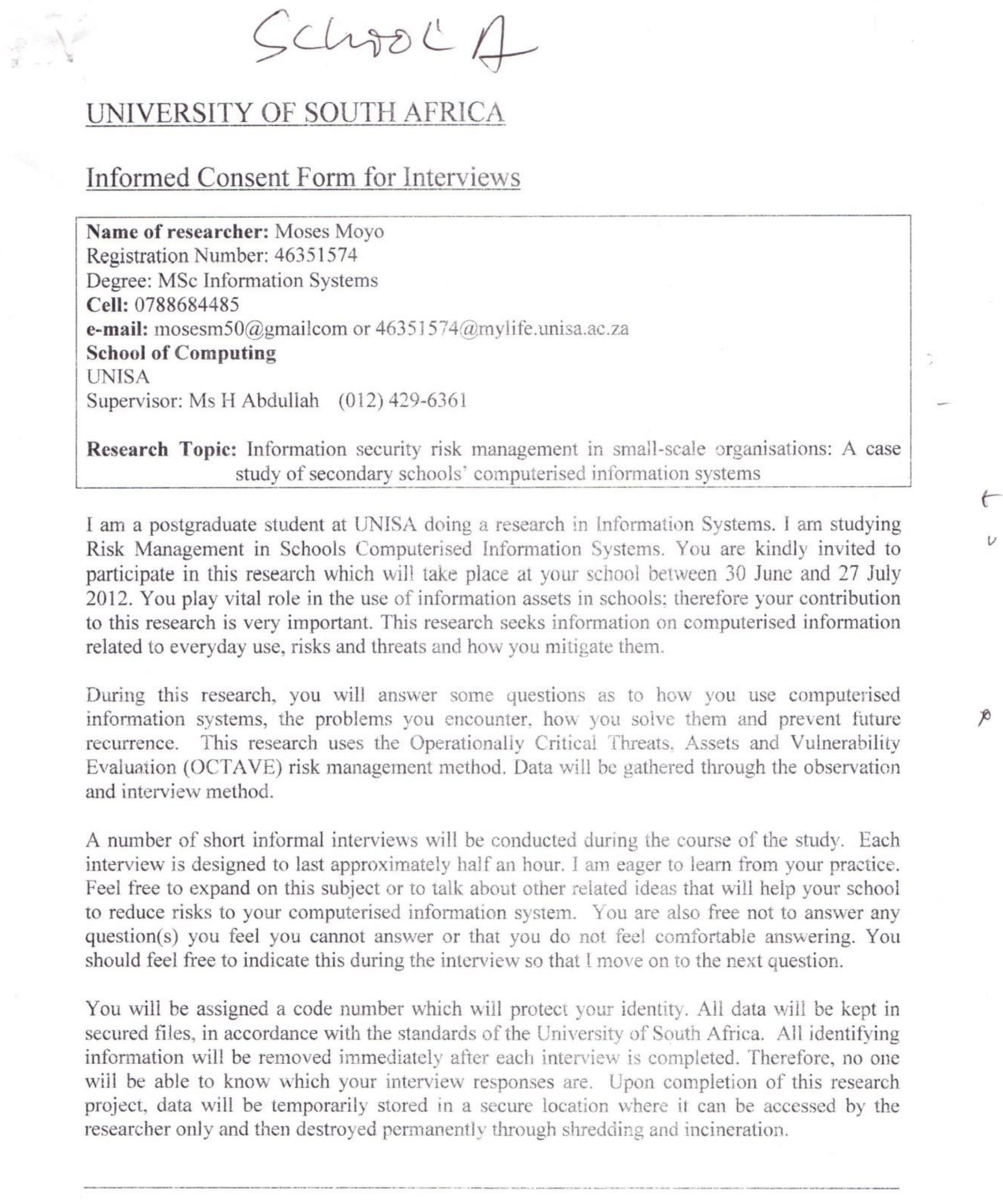
Yours sincerely

Chair: School of Computing Ethics Sub-Committee

University of South Africa
College of Science, Engineering and Technology
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone +27 12 429 6122 Facsimile +27 12 429 6848
www.unisa.ac.za/cset

Open Rubric

APPENDIX 3: SIGNED INFORMED CONSENT FORMS FOR INTERVIEWS



School A

UNIVERSITY OF SOUTH AFRICA

Informed Consent Form for Interviews

Name of researcher: Moses Moyo
Registration Number: 46351574
Degree: MSc Information Systems
Cell: 0788684485
e-mail: mosesm50@gmailcom or 46351574@mylife.unisa.ac.za
School of Computing
UNISA
Supervisor: Ms H Abdullah (012) 429-6361

Research Topic: Information security risk management in small-scale organisations: A case study of secondary schools' computerised information systems

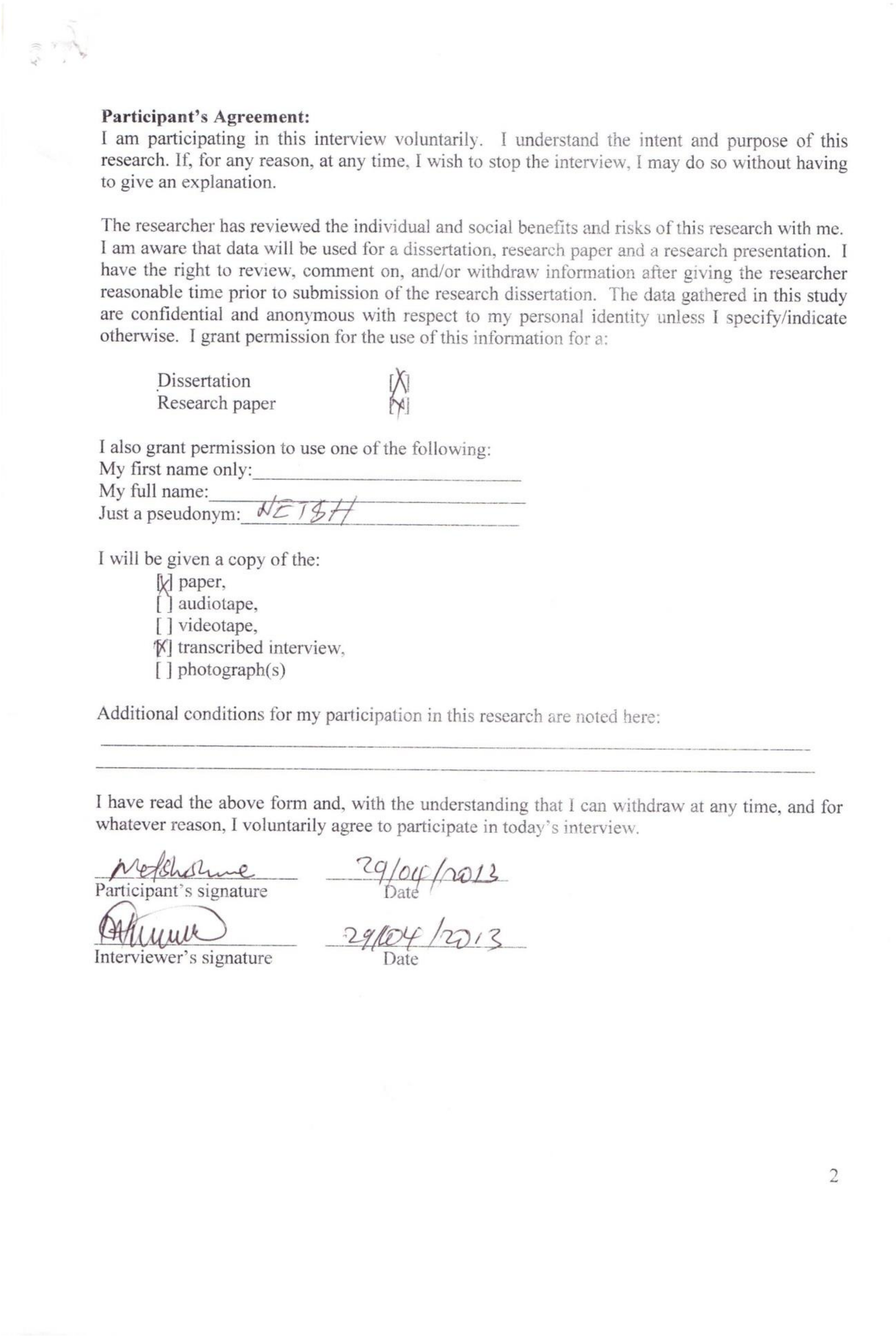
I am a postgraduate student at UNISA doing a research in Information Systems. I am studying Risk Management in Schools Computerised Information Systems. You are kindly invited to participate in this research which will take place at your school between 30 June and 27 July 2012. You play vital role in the use of information assets in schools; therefore your contribution to this research is very important. This research seeks information on computerised information related to everyday use, risks and threats and how you mitigate them.

During this research, you will answer some questions as to how you use computerised information systems, the problems you encounter, how you solve them and prevent future recurrence. This research uses the Operationally Critical Threats, Assets and Vulnerability Evaluation (OCTAVE) risk management method. Data will be gathered through the observation and interview method.

A number of short informal interviews will be conducted during the course of the study. Each interview is designed to last approximately half an hour. I am eager to learn from your practice. Feel free to expand on this subject or to talk about other related ideas that will help your school to reduce risks to your computerised information system. You are also free not to answer any question(s) you feel you cannot answer or that you do not feel comfortable answering. You should feel free to indicate this during the interview so that I move on to the next question.

You will be assigned a code number which will protect your identity. All data will be kept in secured files, in accordance with the standards of the University of South Africa. All identifying information will be removed immediately after each interview is completed. Therefore, no one will be able to know which your interview responses are. Upon completion of this research project, data will be temporarily stored in a secure location where it can be accessed by the researcher only and then destroyed permanently through shredding and incineration.

1



Participant's Agreement:

I am participating in this interview voluntarily. I understand the intent and purpose of this research. If, for any reason, at any time, I wish to stop the interview, I may do so without having to give an explanation.

The researcher has reviewed the individual and social benefits and risks of this research with me. I am aware that data will be used for a dissertation, research paper and a research presentation. I have the right to review, comment on, and/or withdraw information after giving the researcher reasonable time prior to submission of the research dissertation. The data gathered in this study are confidential and anonymous with respect to my personal identity unless I specify/indicate otherwise. I grant permission for the use of this information for a:

Dissertation [X]
Research paper [X]

I also grant permission to use one of the following:
My first name only:____________________________
My full name:__________________________________
Just a pseudonym: NETSH

I will be given a copy of the:

[X] paper,
[ ] audiotape,
[ ] videotape,
[X] transcribed interview,
[ ] photograph(s)

Additional conditions for my participation in this research are noted here:

____
____

I have read the above form and, with the understanding that I can withdraw at any time, and for whatever reason, I voluntarily agree to participate in today's interview.

Metshohne 29/04/2013
Participant's signature Date

29/04/2013
Interviewer's signature Date

APPENDIX 4: SAMPLE OF INTERVIEW TRANSCRIPTIONS

This is the transcript of an interview that was conducted with deputy principal in School A. The interview was tapped using a computer system. This transcript included a number of items shown in normal type face while the responses are in italic type face.

Activity 1: **Asset identification Interview Transcription**

Name of School: ***SCHOOL A*** . Date: ***29 April 2013***
Respondent:… ***Deputy Principal 1***…… Job Description: ***Management***

Part A: Background information

1. **INTERVIER:** How long have you been using school information systems assets?
   DEPT1: I have been using information systems assets for at least 10 years, since 1992.
2. **INTERVIER:** Did you receive formal training in using CISs?
   DEPT1: I only received informal training from the donors of the computers, and the programs we are using. Formal training needs me to go to university or private college**.**
3. **INTERVIER:** Are you familiar with information security risk management?
   DEPT1: Not much but I hear people talk about it just like what you are saying. I know risk management in general, I have never practiced it.
4. **INTERVIER:** What are the information system assets that your school has?
   DEPT: There are so many, some of them I don't know. I will give those I know or use
   a. Computers in the offices.
   b. Mark schedules in the Vanguard program
   c. Information on educators' profiles stored in Excel and Word files
   d. Subject allocation lists for all educators
   e. School termly progress reports on performance of learners and individual educators
   f. Old information on CDs and hard disks of old computers
   g. School fees records in the accountant's computer
   h. The administrator –educator is an important asset.
   i. Router for internet
   j. Wireless network
   k. Computerised asset register, hardware, people

Part B: CISs risk related questions

5. **INTERVIER:** What are the school's important information systems assets you need to protect?
   DEP1:
   a. All computers especially those used for administrative purpose.
   b. Vanguard records program
   c. Subject Allocation lists
   d. Learners' reports schedules in Excel
   e. Back-up disks in the strong room
   f. Payments records in Pastel in the Accountant's computer.
   g. Staff information
   h. Router and the network equipment

6. **INTERVIER:** Where are the identified information systems assets located?

DEPT1:

Asset	Location
a. Computers	Administration block and staff rooms
b. Learners' marks	In the administrator-Educator's computer
c. Staff information	Administrative educator's computer
d. Fee payments	Accountant's Computer
e. Creditor information	Accountant's Computer
f. Router	In the deputy's office
g. Hard copies	In files the administration building
h. Internet equipment	Different offices
i. Application to access CASs marks	

7. **INTERVIER:** Beside the information systems assets you mentioned above, are there any other important information systems assets that your school is should protect?

DEPT1:

a. Printers

b. photocopiers

8. INTERVIER: From the assets that you have identified, which are the most important? What is your rationale for selecting these assets as important?

DEPT1

Asset	**Reason**
a. Computers	The school cannot do without computers. We do all our work computers
b. Vanguard system	It's handy in data capturing, processing and printing reports.
c. Learners' CASS marks in Vanguard database	These marks are needed every year to promote learners at the end of the year
d. Creditors payments information	If this information is not available, we may pay double.
e. Router or modem	Connects to the internet
f. Network	Enables us to connect to computers in other offices.
g. Staff information	This information is used for administration

9. **INTERVIER:** What have been the security issues since you started using computerised information system in terms of:

a. Hardware failures

DEPT1: I have computers many times. Sometimes it is very slow does not open files. It gives a blue screen or keeps on restarting. One day I found out that my hard disk was damaged. I lost all important information. I had to restart typing all information from hard copies, but with Vanguard system, we cannot retype every lost mark. Some CDS do not open at all.

b. Software failure

   i. Operating systems

      DEPT1: My computer has been erased so many times because of hanging. I did not know the problems behind that, but the administration educator attended to it. At time it could not shut down when I tried to shut it down. Once the information on the hard disk is erased it becomes difficult to run the school and attend to learner's problems especially those that pertain to marks.

   ii. Specialised software

      DEPT1: Vanguard is reliable most of the time. However, if the computer is not working well it gives us problems. It may not load or miscalculates the figures.

   iii. Generic applications

      DEPT1: There are very few problems. Only that some old files are difficult to open on the new Excel or Word. They give unreadable characters.

c. Loss of data integrity, confidentiality or availability through intentionally or unintentionally operations due to

   i. your actions

      DEPT1: I forget to close my files when I leave the office to supervisor classrooms. Some users who happen to get to my office at times read the information. Some of it would be confidential. At times I accidentally delete files or save using the same name. I tried to undo but it is difficult once you save using same name. At times I forget the file names and lose them and vital information. I also misplace hard copies and never recover them. I suspect that someone could be taking them but I cannot tell.

   ii. other authorised internal users

      DEPT1: During printing, users mix up and print my open files and take away the hard copies. Some of the users are eager to change learner's marks on the mark schedules if they can get a chance. There are situations when there are unaccountable changes in some marks of learners. Vanguard uses one password. Once it leaks, it is possible for these some of the users to change information. If someone opens and file and changes information, then its intentional.

   iii. unauthorised internal users

      DEPT1: I miss a lot of documents, soft copies and hard copies through unauthorised users who enter my office and use my computer. These people know all my movements. When I come in I do not find them. I cannot lock my office during the day people will think I will be absent.

   iv. your superiors

      DEPT1: The principal does not use this computer. He has access to Vanguard, but we do not know the changes he makes on the mark schedules if any. But I do not think that he does so.

v. external users

DEPT1: Normally we do not allow external users to use our computers or have access to any information assets except if the person is hired by the school.

vi. malware

DEPT1: This is a headache. We have big problems with virus. They come from outside with users in their memory sticks. I have a lot of files which cannot open or they open but with missing information. At times computers have to be formatted because of virus problems.

vii. hacking

DEPT1: I have no idea about tis. You better the Administrative educator.

viii. Unaccountable factors

DEPT1: At times my computer switches restarts on its own. I lose my files when it restarts. I have experienced this for some time.

10. **INTERVIER:** How severe did these have on the operations of the school?

DEPT1: The school delays in sending schedules or printing reports. At time we may have to conduct meetings with sufficient documents. This affect decisions to be made at the same time the operations are severely affected especially if CDs containing tests fail to open, we suspend the tests and rescheduling is difficult again. Think of a situation the file with the five mark schedule disappearing and retyping it.

11. **INTERVIER:** Can you briefly describe how you responded to each of these problems?

DEPT1: The Administrative educator try to solve the problems related to computers. I work on those related to hard copies in trying to save the situation. At times we resort to hard copies and backups where possible. If the situation cannot be redressed, we hire a technician to help.

12. **INTERVIER:** What measures do you put in place to secure your workstation when you go out for a break?

DEPT1: There is no mechanism I use for this computer. There are many people who want to use it for printing.

13. **INTERVIER:** In what condition do you find your workstation when you return from your break?

DEPT1: I do not take this seriously. Sometimes I find it open or someone using it. Files could be closed or open. Some files could be missing and find them in the recycle bin

14. **INTERVIER:** Do other computer users in school temper with your computer during at any time during your presence absence

DEPT1: Yes, they use it especially those who want to print. Some used to access internet from my computer.

15. **INTERVIER:** What activities do these perform on your computer?

DEPT1: Printing, searching internet

16. **INTERVIER:** How do you check whether your computer or data has been tempered with?

DEPT1: No. I am too busy to do that. I expect it to be in perfect condition.

17. **INTERVIER:** Do you access to internet on your work station?

DEPT1: Yes.

18. **INTERVIER:** What data recovery method do you use in the event that your computer has crashed?

DEPT1: I do not have any mechanism except using backups. Otherwise I retype all the information.

19. **INTERVIER:** What do you do if your computer is infected by a recently deployed virus?
DEPT1: I do not know what to do. I ask the admin educator to help.

20. **INTERVIER:** What would you do if pirated software is installed on your computer?
DEPT1: Do you think I know what is which software is pirated or not? I just use what is there.

21. **INTERVIER:** What problems have you encountered with your CISs?
DEPT1: We lose information due to viruses and hardware problems. We may delay in processing of school reports or even entering data. Sensitive information is read by those who are not supposed to read it.

22. **INTERVIER:** How frequent has each of the problems been?
DEPT1: I can say many times. It is difficult to say how many times. But it happens. I cannot remember because it occurs when we are so busy that you focus on finishing the work.

23. **INTERVIER:** What initiative has been made to:
    a. Solve the problem
    DEPT1: Not much has been done. No one is competent enough to deal with the situation. Even though, we want things got done and then we move on.
    b. Prevent the problem to occur again
    DEPT1: Do you think there is a way to prevent this? Because the problem may be even bigger immediately after a technician has attended to it. When you try to prevent viruses, some users who do not know bring them into the school.

24. **INTERVIER:** How effective was the initiative made in
    a. Solving the problem
    DEPT1: There is no effective solution. I think we need to training everyone who use computers on the issue of viruses and not deleting other people’s files.
    b. Preventing it from recurring?
    DEPT1: the school has no mechanism for this.

25. **INTERVIER:** Do you have full user rights for all customised software?
DEPT1: I do not think so. I do not have because I cannot change anything even reinstallation. Were rely on the suppliers

26. **INTERVIER:** How do you deal with those important files which do not open?
DEPT1: If there are important, we try our level best to open them using various programs. But if we fail, we retype the important information and save it correctly

27. **INTERVIER:** What would you do if your hard disk fails?
DEPT1: I refer everything to the Administrative educators. He is the one who will replace it or try to repair it.

28. **INTERVIER:** Do technicians attend to your computer in your presence?
DEPT1: No, they either take the computer to their workshops or other private space. They do not want us to see what they are doing. At times I do not want to be disturbed they have to work somewhere

29. **INTERVIER:** How secure is your CISs from
    a. internal intruders
    DEPT1: I do not think it is secured. I am not sure.
    b. external intruders
    DEPT1: we do not have such people around.
    c. unexpected hardware crashes
    DEPT1: it is not secured because we lose such information every time. Normally t is replaced with a new one.

30. **INTERVIER:** What mechanisms do you use to detect intrusions in your CISs?
DEPT1: Nothing in place at all. May be as times goes on will find the appropriate ones.

31. **INTERVIER:** What methods of backups do you use and where do you store them?
DEPT1: we use CDS, Memory sticks, DVDs, hardcopies. CDs are in the strong room. I have my memory stick every time.

32. **INTERVIER:** How do you deal with virus problems?
DEPT1: I refer this matter to Administrative educator who attends to it. Some I clean if it is easy or technicians are hired for this purpose if we have money.

33. **INTERVIER:** What challenges do you face in securing your CISs?
DEPT1: They are many. In the CASs mark database we use the same password. Locating some information could be difficult at times. Forgetting of password is also a problem.

APPENDIX 5: RISK IMPACT EVALUATION CRITERIA

Table AP3.1: OCTAVE-small- Risk Impact Evaluation Criteria

Impact Area	High	Medium	Low
Reputation of school Confidence of creditors, parents and learners, education authorities	• Reputation irrevocably destroyed or damaged • Rating of school by district and drops drastically. School placed under strict circuit and district supervision • Creditors unpaid for a long period due to missing records	• Reputation damaged; some effort and expense required to recover • Reduction or warning of reduction of rating or accreditation by authorising organisations	• Reputation minimally affected; little or no effort or expense required to recover • No change in rating or accreditation by authorising organisations
Productivity	• School management fails to meet obligations because information is inaccessible due to systems which are down. • Critical asset is completely rendered useless and valuable data/information is irrecoverable • Asset very difficult to replace • Irrecoverable loss of learner records/information • The system is completely paralysed and school decides to abandon its use • Fails to print reports completely.	• School management delayed in meeting obligations while the system tries to recover from threat effects. • Increases in general staff work of 10-40% for one day (duplicating written records, recapturing marks, re-creating mark schedules, retrieving and verifying back-up data) • Slow in printing relevant documents misplaced information	• Simple inconvenience school management that last few hours on matters of little importance • No measurable increase in the amount of work to be done in data capturing and redoing mark schedules. • No noticeable delays in submitting administrative documents to circuits. • Parents wait while reports are being printed • Creditors just inconvenienced for less than a day in getting their payments
Finances	• School loses 10% yearly revenue in replacing stolen or damaged hardware • School suffers 10%	• School loses 5% yearly revenue in replacing stolen or damaged hardware • School loses 5%	• School loses 1% yearly revenue in replacing stolen or damaged hardware • School loses 1%

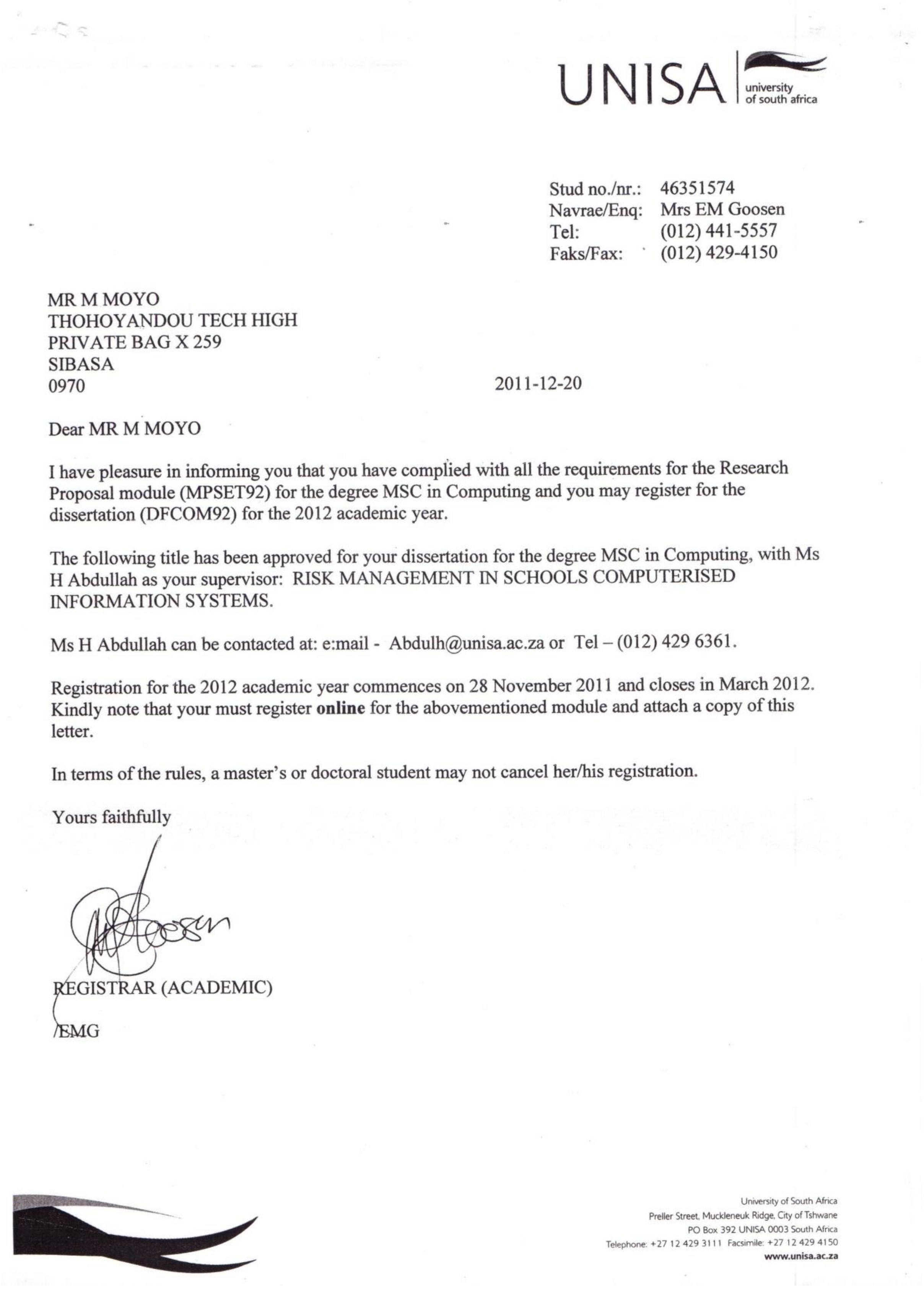
	yearly revenue loss due records modification, misplacements or destruction. • School suffers 5% yearly financial cost malware in cleaning by hired personnel.	yearly revenue in replacing stolen or damaged hardware • School suffers 5% yearly revenue loss due records modification, misplacements or destruction. • School suffers 2% yearly financial costs in malware cleaning by hired personnel. • Partially correctable errors in funding and personnel	yearly revenue in replacing stolen or damaged hardware • School suffers 1% yearly revenue loss due records modification, misplacements or destruction. • School suffers negligible yearly financial cost in malware cleaning by hired personnel. • Inconvenient but correctable errors in funding and personnel
Other (Facilities)	• Loss of an entire facility or building due to fire • False software or service providers	• Damage to a facility or building requiring temporary relocation computing records management systems • Unable to verify credentials of providers software service providers • Unable to track performance of facilities or providers accurately	• Loss of air conditioning for two weeks • Negligible impact on daily operations

APPENDIX 6: DATA COLLECTION ACTION PLAN

Table AP6.1: Data Collection Action Plan for both schools

Activity	**Date**	**School**
First collaborative team workshop	22 April 2013	School A
	24 April 2013	School B
Interviews Deputy principals and Administrative educators	29 April 2013	School A
	06 May 2013	School B
Second collaborative team meeting	10 May 2013	School A
	10 May 2013	School B
Inspection of assets	13 May 2013	School A
	14 May 2013	School B
Critical Assets identification meeting	15 May 2013	School A
	16 May 2013	School B
Current threats Identification And Security requirements meeting	20 May 2013	School B
	21 May 2013	School A
Identifying Vulnerability in Technology workshop and physical testing	23 May 2013	School B
	24 May 2013	School A
Risk identification, analysis and Evaluation workshop	25 May 2013	School A
	27 May 2013	School B
Mitigation strategies and plans meeting	30 May 2013	School A
	31 May 2013	School B
Winding up data collection and meeting	04 June 2013	School A
	05 June 2013	School B

APPENDIX 7: LETTER OF ADMISSION TO DINF91



UNISA university of south africa

Stud no./nr.: 46351574
Navrae/Enq: Mrs EM Goosen
Tel: (012) 441-5557
Faks/Fax: (012) 429-4150

MR M MOYO
THOHOYANDOU TECH HIGH
PRIVATE BAG X 259
SIBASA
0970

2011-12-20

Dear MR M MOYO

I have pleasure in informing you that you have complied with all the requirements for the Research Proposal module (MPSET92) for the degree MSC in Computing and you may register for the dissertation (DFCOM92) for the 2012 academic year.

The following title has been approved for your dissertation for the degree MSC in Computing, with Ms H Abdullah as your supervisor: RISK MANAGEMENT IN SCHOOLS COMPUTERISED INFORMATION SYSTEMS.

Ms H Abdullah can be contacted at: e:mail - Abdulh@unisa.ac.za or Tel – (012) 429 6361.

Registration for the 2012 academic year commences on 28 November 2011 and closes in March 2012. Kindly note that your must register **online** for the abovementioned module and attach a copy of this letter.

In terms of the rules, a master's or doctoral student may not cancel her/his registration.

Yours faithfully

REGISTRAR (ACADEMIC)

/EMG

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za