Information Security Assurance Model for an Examination Paper Preparation Process in a Higher Education Institution

By

Miemie Mogale

Submitted in fulfilment of the requirements for the degree
Magister Technologiae

in

Information Technology

in the

FACULTY OF ENGINEERING, THE BUILT ENVIRONMENT
AND INFORMATION TECHNOLOGY

at the

NELSON MANDELA METROPOLITAN UNIVERSITY

Supervisor: Prof. Mariana Gerber

Co-Supervisor: Prof. Rossouw von Solms

March 2016

DECLARATION

I, **Miemie Mogale (210235292)** hereby declare that the dissertation for Masters: Information Technology is my own work and that it has not previously been submitted for assessment or completion of any postgraduate qualification to another University or for another qualification.

... . (Signature)
Miemie Mogale

ACKNOWLEDGEMENTS

I thank the Lord Almighty for the blessings bestowed upon me and for the strength to persevere. Moreover, I thank Him for the following people who have provided me with the support I needed.

- My supervisor, Prof Mariana Gerber & co-supervisor, Prof Rossouw von Solms for their informed professional & competent guidance, advice, continual support and commitment.

- My loving family for their motivation, encouragement and loving support through it all.

- My friends and colleagues for their keen interest, advice and encouragement.

- The National Research Foundation (NRF), Nelson Mandela Metropolitan University (NMMU) Research Capacity and Development as well as Standard Bank for the financial assistance. Opinions expressed and conclusions arrived at, are those of the author and not necessarily to be attributed to the organization.

I dedicate this dissertation to:

My loving mother, Nomvula Mohlokoana. Thank you very much for always believing in me, encouraging me and always pushing me to greater heights.

ABSTRACT

In today's business world, information has become the driving force of organizations. With organizations transmitting large amounts of information to various geographical locations, it is imperative that organizations ensure the protection of their valuable commodity. Organizations should ensure that only authorized individuals receive, view and alter the information. This is also true to Higher Education Institutions (HEIs), which need to protect its examination papers, amongst other valuable information.

With various threats waiting to take advantage of the examination papers, HEIs need to be prepared by equipping themselves with an information security management system (ISMS), in order to ensure that the process of setting examination papers is secure, and protects the examination papers within the process. An ISMS will ensure that all information security aspects are considered and addressed in order to provide appropriate and adequate protection for the examination papers.

With the assistance of information security concepts and information security principles, the ISMS can be developed, in order to secure the process of preparing examination papers; in order to protect the examination papers from potential risks. Risk assessment form part of the ISMS, and is at the centre of any security effort; reason being that to secure an information environment, knowing and understanding the risks is imperative. Risks pertaining to that particular environment need to be assessed in order to deal with those appropriately. In addition, very important to any security effort is ensuring that employees working with the valuable information are made aware of these risks, and can be able to protect the information.

Therefore, the role players (within the examination paper preparation process (EPPP)) who handle the examination papers on a daily basis have to be equipped with means of handling valuable information in a secure manner. Some of the role players' behaviour and practices while handling the information could be seen as vulnerabilities that could be exploited by threats, resulting in the compromise in the CIA of the information. Therefore, it is imperative that role players are made aware of their practices and

behaviour that could result in a negative impact for the institution. This awareness forms part and is addressed in the ISMS.

Table of Contents

List of Figures

List of Tables

Chapter 1

INTRODUCTION

1.1 Prologue

The purpose of this chapter is to provide an overview of the research study, by providing the background that led to the development of the study (Section 1.2). The background is followed by the description of the problem area (Section 1.3), followed by the problem description (Section 1.4), leading to the problem statement (Section 1.5). Following the problem statement is the presentation of the research objectives (Section 1.6). Subsequently, the research methodology is discussed (Section 1.7). This is followed by the delineation (Section 1.8); ethical considerations (Section 1.9); dissertation chapter overview (Section 1.10) and finally, the chapter conclusion (Section 1.11).

Having presented the overview of the chapter, the chapter will commence with the background.

1.2 Background

Higher Education (HE) is an educational level that follows grade 12 (Minister of Education, 1997). Teaching, learning and research is core to HE, and is intended to supply high-level skills for the labour market, and to generate knowledge that is of social and economic benefit (Department of Education, 1997). In South Africa (SA), HE has come to play a vital role in defining a democratic society, which addresses and promotes human dignity, equality and freedom (Minister of Education, 1997). It plays a central role in the social, cultural and economic development of the nation (Department of Education, 1997). According to the Ministry of Education (2001), the goal of HE is to:

- Contribute to the social, economic, cultural and intellectual life of a rapidly changing society, by mobilising human talent and potential, through life-long learning.

- Ensure national growth and competitive edge - which is dependent on continuous technological improvement and innovation - by producing, acquiring, and applying new knowledge, through a well-organised research and development system.
- Strengthen the enterprise, service and infrastructure of the country, by training and establishing human power, through the development of professional and knowledge workers with globally equivalent skills.

The efficiency and effectiveness of HE is evident in the overall quality of graduates produced by the various Higher Education Institutions (HEI). This depends on the quality of education, skills and knowledge produced, as well as on the management, leadership, and governance of the institutions (Ministry of Education, 2001).

HEIs are institutions that provide HE; they are the vehicle through which the goals of HE are achieved. According to the South African Students Congress (SASCO) (2009), HEIs are an environment for teaching, learning and research, and are responsible for creating new knowledge and for transmitting that knowledge to students and future generations. SASCO further elaborates that HEIs are responsible for producing skills and knowledge that will meet the economic and social requirements of the nation. HEIs need to ensure that the skills and knowledge imparted to students are responsive to the ever-changing influences of the external environment, and should, therefore, promote the development of a nation committed to life-long learning and advancement (Shapiro, 2005). This will ensure that the responsibilities placed on HEIs respond to and meet the economic and social requirements of the nation. In order for HEIs to meet their responsibilities, they have to be accountable to the public, by producing knowledgeable graduates with high-quality skills and competencies in all prospective fields of study (SASCO, 2009; Ministry of Education, 2001). That is, produce graduates who will be able to meet the needs of industry and social reconstruction.

In SA, HEIs are categorized and recognized as universities, comprehensive universities and universities of technology (Council of Higher Education, 2009). Recently, these institutions have become autonomous organizations: which refers to their “administrative independence with respect to the internal management of resources, methods of teaching and assessments, curriculum and student admissions” (Department of Education, 1997). There has also been an increased competition amongst the various HEIs, owing to financial constraints as a result of limited financial resources (Ministry of Education, 2001). The institutions rely primarily on three sources of funding: government funding, student fees and third stream income (Council of Higher Education, 2009). Owing to limited funding, HEIs are continuously seeking new ways of generating supplementary third stream income, through donations, investments and entrepreneurial activities (IEASA, 2011). With a good reputation, HEIs have a good standing for attracting huge amounts of third stream income. According to the Ethics Resource Center (2011), a good reputation is a valuable commodity for any organization, as it helps in securing investments and attracting customers.

It can be deduced that the reputation of HEIs play a vital role in securing third stream income, as well as in attracting students who contribute financially through the payment of student fees. According to SASCO (2009), in order to maintain their reputation and to ensure that they remain credible, the various HEIs need to, amongst other things, ensure that they:

- provide high quality education;
- produce high quality teaching and learning outcomes;
- promote ethical behaviour and professional integrity, by dealing strictly with the unethical behaviour of their students and staff;
- are not undermined, owing to the knowledge, skills, and expertise they provide being in question.

Therefore, it is essential that the HEIs ensure that their reputations are maintained. This could be achieved, amongst other things, by ensuring that the qualifications they award are credible and never questionable. The reason for saying this is that institutions are responsible for maintaining academic standards and for performing according to the quality assurance standards set by the Higher Education Quality Council (HEQC) and the South African Qualifications Authority (SAQA) respectively. A further reason is that institutions are responsible for maintaining the quality assurance for the qualifications that they award (NUI, 2007). Hence, it is crucial that institutions deal with intellectual property protection and academic integrity, amongst others, which are under constant media and public scrutiny (Sutherland-Smith, 2008). A possible reason for this could be that institutions are seen as intellectual communities which are based on the creation, transmission, sharing and applying of knowledge, through their intellectual property and academic standards (Ministry of Education, 2001). One way of ensuring that the qualifications awarded are credible, is to ensure that the qualifications are awarded to deserving students, students who have demonstrated competence in the achievement of the learning outcomes of a module. In order to gain evidence of the competence of students, institutions rely primarily on examinations.

Examinations assess the knowledge of a student to give assurance that the student has sufficient understanding of that which is being assessed. For educational institutions such as universities, an examination is an assessment method that collects evidence of the competence of a student to demonstrate the achievement of the learning outcomes of a module (NMMU, 2011). Examinations could thus provide assurance to future employers that the passing students have an understanding of what is being presented in a module and have mastered the study unit (Assessments are discussed further in Chapter 3).

However, if there is ease by which examination papers are illegally obtained by students, this will create a cheating environment, where students do not apply themselves to their studies to learn and gain the necessary knowledge and skills. As a result, owing to their lack of knowledge and skills, their abilities could be questioned in the industry, thereby questioning the qualifications issued by the institutions from which they had graduated. Thus, when examination papers are accessible to unauthorized persons, it not only undermines the integrity of the examination process, but of the institution as a whole. Hence, it may cost the institution its credibility in the industry, if students pass and obtain qualifications without demonstrating the required level of understanding and basic knowledge (Knowledge@ W.P Carey, 2008). Universities should, therefore, ensure that academic dishonesty is prevented and detected. The confidential information and intellectual property of the institution, such as examination papers should, therefore, be adequately protected, in order to protect the credibility of honest and hardworking students, as well as the reputation of the institution. This will ensure the continued integrity of the degrees and qualifications of the institution (University of Toronto, 2009). Higher education institutions are, therefore, responsible for ensuring that an effectively controlled and secure examination process is in place. To exercise control, the examination process needs to be properly managed.

In most higher education institutions, the Examination Office is, to a large extent, mostly relied upon to operate and manage the examination process in a professional and efficient way. The Examination Office is further responsible for the central administration of the examination process of that institution, which includes, amongst others, the development and implementation of procedures and processes for the preparation and administrative support of examinations (NUI, 2007). The purpose of the Examination Office is, therefore, to ensure that there is an efficient and effective examination process in place, and that the process safeguards and maintains the academic integrity of examinations (York University, 2007). Part of this lies in ensuring that there is a secure process for preparing examination papers, and that during the process, the examination papers are well protected.

The process of preparing the examination papers, referred to as the Examination Paper Preparation Process (EPPP) in this research study, is the starting point of the examination process. The EPPP includes the compilation and storage of the examination papers and memoranda (this will collectively be referred to as examination papers), as well as the transmission of those amongst the examiners, the internal moderators, the academic heads of departments (HODs), and the examination officers at the Examinations Office. For the purpose of this study, the external examiners and external moderators are excluded, as they fall beyond the scope of this study.

1.3 Problem Area

We now live in the ‘information age’ - also commonly known as the ‘computer or digital age’. Today, the internet has become the ultimate platform for the flow, transmission and exchange of information. The connectivity of computers poses a facility for workers to access and share information more easily, hence, the ‘information age’, and new technologies have become available to expedite the use and dissemination of information. This has led to the expansion of information and communications technology (ICT) (Todd, 2007). In the ‘information age’ most organizations rely on ICT to conduct their operations efficiently. ICT, through networked computing, which connects computers and other electronic devices via communication networks, has allowed users to communicate and collaborate on projects using methods such as emails, voice mails and computer conferences, amongst others. With new developments in ICT, employers are now able to work from remote locations, with the use of mobile devices (such as laptops and iPads) and other mobile storage devices (e.g. flash drives and external hard dives). ICT has provided convenience and improvement in productivity. However, if not used responsibly and securely, the information processed, stored and transmitted using ICT could be at risk. The risk could arise from the loss of confidentiality, integrity and availability of the information or information systems; due to the unauthorized access to the information or information systems (ISO/IEC 31000, 2009) Although there are various security controls that could be implemented to protect the information against risk, the human element is one of the challenges facing efforts to secure information. Human behaviour and practices are often seen as security concerns which need to be addressed appropriately, as human behaviour is referred to as the weakest link in information security (Posthumus & von Solms, 2004).

As with most organizations and their employees, universities and their employees use ICT for many of their operations. For example, examiners use computers and laptops to compile their examination papers. They then use mobile storage devices to store the examination papers for later retrieval, backup purposes or to work from home. Communication methods such as emails are used to transmit the examination papers amongst each other when collaborating on the examination papers. The use of ICT assists examiners in preparing their examination papers in an efficient, convenient and productive manner. However, it is imperative that examiners ensure that the examination papers are well protected while using ICT. Examination papers are the confidential information of the institution that needs to be protected at all times and should not be accessible to unauthorized persons. It is imperative that examination papers be properly protected, in order to ensure that the integrity and confidentiality of the entire examination process is protected, so as to safeguard the reputation of the institution.

Ensuring that examination papers are secure is not the sole responsibility of the Examinations Office, but the responsibility of everyone involved in the EPPP. After all, as Whitman and Mattord (2008) state, security is the responsibility of every employee. The Examinations Office may ensure that the policies and procedures are in place, to guide actions towards achieving desired outcomes and practices for a secure process, but everyone else involved needs to follow these policies and procedures, to ensure secure practices and the secure handling of examination papers. From the start of the EPPP, every person involved is responsible for preserving the confidentiality, integrity and availability (CIA) of the examination papers. Therefore, every person needs to adhere to the implemented policies and procedures in order to ensure that the process is secure and that the CIA of the examination papers is preserved.

1.4 Problem Description

Quite often, role players in the EPPP (examiners, moderators, HODs, and examinations officers), while going about their daily activities during the process, may lack security considerations when it comes to their practices. They might not be aware that their daily practices and behaviour could be potential vulnerabilities in the process. The role players may be unaware that what they are doing could compromise the security of the examination papers and the entire EPPP. Role players might be performing their day-to-day activities, only thinking of getting the examination papers completed on time, without being conscious of any security-related issues, especially with the use of ICT. However, without being aware of their unconsciously negligent practices and without taking security into consideration, this could lead to a serious security breach, thus placing the examination papers and the process in jeopardy and at risk. The security of the examination papers could be compromised by overlooking just a single vulnerability that may be exploited by a threat. Such vulnerabilities may include, for instance:

- Offices and computer screens left unlocked and unattended. If at that time the role players were working on examination papers, intruders could gain access to the offices, therefore having access to the examination papers.
- Not keeping backups of the examination papers. If by any chance the single copy of the examination paper gets corrupted or lost, this might compromise the availability of the examination paper, should the paper be needed and there is no backup copy.
- Not encrypting (password protect) examination papers. Should the mobile devices of the examiners, on which the examination paper is stored, end up in unauthorized hands, it will mean that the unauthorized person could have access to the examination paper with ease. Without encryption of the examination papers, they could also be intercepted while being emailed.

Other vulnerabilities could include:

- Not being aware of the examination policy (which is meant to direct the examination process, including the secure preparation of examination papers).
- The inadequacy of the examination policy in addressing relevant security issues (this may lead to role-players not being aware of what is expected of them, as well as not being equipped to deal with the security issues not addressed by the policy).

These are just a few examples of what could compromise the security of the examination papers. The full extent of these vulnerabilities is explored in detail in Chapter 4.

Most people might be under the impression that examination papers are not being compromised owing to the lack of knowledge about such breaches. However, it does not mean there are no breaches just because there are no such reports; this may just be the result of the perpetrators not having been caught. Therefore, it is crucial to ensure that the EPPP is secure and that all possible vulnerabilities are dealt with; ensuring that there are no opportunities for exploitation. Ensuring the security of examination papers will assist the credibility of the institution; rather than having the institution deal with stakeholders and the media, or having to do damage control, once the reputation of the institution has been tarnished.

Whenever the role players prepare examination papers, they should take note of their practices while processing (compiling), storing and transmitting the examination papers. The role players should also be aware of and should adhere to the relevant policies and procedures. In doing so, they could eliminate possible vulnerabilities, which could be detrimental to the examination papers and the EPPP. The Examinations Office should therefore ensure that the EPPP is properly controlled and that information security is a priority, by ensuring that vulnerabilities are appropriately addressed, in order for the examination papers to be properly protected. Information security is about preserving the CIA of information and information systems (Whitman & Mattord, 2008). The Examinations Office should also ensure that role players are aware of what is expected of them regarding the security of the examination papers, and the secure use of ICT while preparing the examination papers. The Examinations Office should thus ensure that the EPPP is well controlled and managed, with all necessary information communicated to all role players, in order for them to be aware of what is expected of them. The Examinations Office should try to adopt a system that will assist in controlling and managing the security of the EPPP, a system which will aspire to improve the security of the examination papers.

Most organizations rely on a well controlled and managed information security system to help guide in ensuring that their valuable and confidential information is suitably and appropriately protected (ISO/IEC 31000, 2009). Such a system ensures that relevant and appropriate policies are in place to control: practices, behaviour, processes, as well as the use of ICT (Von Solms & Von Solms, 2004). In addition, the information security system ensures that proper communication of the policies is in place. This will ensure awareness of issues addressed in the policies, which, in turn will assist in promoting compliance. From the previous discussion, it can be deduced that certain of the practices and behaviour of examiners pose potential vulnerabilities that need to be addressed. Additionally, not having adequate policies in place may contribute to the security of examination papers being compromised. These are security issues that need to be addressed in order to ensure a secure EPPP that protects the examination papers. Thus, it can be reasoned that such a system is required to address and manage these security issues concerning the EPPP.

1.5 Problem Statement

From the problem description discussed, it becomes clear that the security oversight and the current manner in which examination papers are being prepared, may lead to the security of those papers being compromised.

Therefore, the problem addressed in this research study is the current uncontrolled and unmanaged manner in which examination papers are being prepared (compiled, stored and transmitted) by role players, which could compromise the security and integrity of the EPPP, the examination process, and the reputation of the university as a whole.

1.6 Research Objectives

With a well controlled and managed system required to ensure that the examination papers are protected adequately, this research study aims to propose a model for managing and improving security during the process of preparing examination papers.

The primary objective of the research is:

- To propose a model for managing and improving security and for the secure use of ICT during the Examination Paper Preparation Process at a higher education institution.

The following are the sub-objectives:

- To determine the current security state of the Examination Paper Preparation Process at a particular higher education institution, including identifying policies and procedures relevant to the process.
- To identify relevant information security aspects and applicable information security principles from existing information security best practice frameworks and standards that need to be considered, to contribute towards a secure Examination Paper Preparation Process at a higher education institution.
- To integrate the identified information security aspects and information security principles, in order to contribute towards the development of a model for managing and improving the security of the Examination Paper Preparation Process at a higher education institution.

1.7 Research Methodology

Research is described by Graziano and Raulin (2000), as a process of inquiry, a systematic search for information. Defined by Saunders, Lewis and Thornhilll (2007), research is “the systematic collection and interpretation of information with a clear purpose to find out things”. When undertaking a research study, a plan, structure and strategy on investigation is conceived. This will provide guidance on how to address the research problem in order to achieve the set objectives (Lincoln & Guba, 1985). To reach the set objectives, various appropriate research methods are incorporated to collect the required data needed to find out things. Owing to the nature of the data this research study was aiming to collect and use, the following research methods were employed: a literature review, interviews, questionnaires, observation, document review and argumentation. In addition, a qualitative approach was followed and a case study strategy applied.

According to Anderson (1998), a **qualitative approach**, is a form of inquiry that explores phenomena in their natural setting and uses multi-methods to interpret, understand, explain and bring meaning to them.

In the case of this research study, the role practices of the role players while preparing examination papers were explored in order to interpret those practices and to obtain an understanding with regard to information security.

A **case study strategy** was applied in conducting this research study. A case study is a holistic research strategy that uses multiple sources of evidence to analyse or evaluate a specific phenomenon (Anderson, 1998).

For this research study a case study was applied to enquire about the practices of role players when preparing examination papers at the Nelson Mandela Metropolitan University (NMMU), in terms of compiling, storing and transmitting the examination papers.

According to Henning (2004), in a case study a phenomenon is investigated as a "bounded system", which "system" may be a group of people; it may also be a set of documents.

For this research study the "bounded system" investigated was both a group of people (the examiners, moderators and examinations officers at NMMU), as well as a set of documents (the documented examination policy and procedures).

Anderson (1998) further states that a case study is concerned with how and why things happen, allowing the investigation of contextual realities and the differences between what was planned and what actually occurred.

Through the interviews and questionnaires, this research study investigated how examiners and moderators prepared and moderated the examination papers. It investigated their practices when compiling/moderating, storing and transmitting the examination papers. It further investigated, through observation, how the examination officers accepted the examination papers from the examiners. This was then compared to what is expected, based on a review of the documented examination policy and procedures, in order to identify the actual practices versus the documented expected practices. This also assisted in identifying the shortfalls of the documented policy regarding what is expected of role players during the EPPP.

As mentioned earlier in this section, a literature review, interviews, questionnaires, observation, document review and argumentation were employed for data collection. The next section discusses these methods in more detail. In Chapter 4 the results of these methods will be discussed as part of the output of the EPPP assessment.

1.7.1 Research Methods

A **literature review** is a comprehensive study of available literature through a variety of sources (White, 2010). It is undertaken to study the relevant field and to provide an overview of that field or an aspect of that field (Hofstee, 2006).

For this research study, the literature review included literature on:

- HE, HEIs and the examination process - to gain insight into the subject matter of this research study. To understand the importance of HE, the role that HEIs play and the importance of the examination process within the HEIs;
- information security - to gain an understanding of the importance of information security in protecting valuable information;
- information security risk assessment – to understand the purpose and how it contributes in ensuring security of information;
- information security management systems - to understand the purpose in terms of the management and control of information security and to identify essential information security aspects that need to be considered to ensure a secure EPPP; as well as
- information security international best practices - in order to determine applicable information security best practices that can contribute to the development and implementation of an adequate model for improving the security of the EPPP.

Interviews and questionnaires are a form of surveys used to elicit information from the people who are presumed to have the required information (Hofstee, 2006). **Interviews** are usually conducted to "understand the phenomenon of interest from the individual perspectives of those who are involved in it" (Henning, 2004). They are conducted to gain insight into certain issues. The positive aspect of interviews is that the researcher can gather reliable information relating to the problem being investigated, as well as that the researcher is able to probe for more information if the need arises (Hofstee, 2006). However, there are also negative aspects to interviews. Interviews can tend to be biased, as interviewers can lead the interviewee in giving the answers that they want. In addition, the interviewee may react to the perceived character of the interviewer, thereby influencing the answers (Hennink, Hutter, & Bailey, 2011). According to Hofstee (2006), interviews may be structured, unstructured or semi-structured. Structured - interviewees are asked the same questions with the same optional answers; unstructured – questions may be different for interviewees and they have an option of answering as they see fit; semi-structured – depending on the circumstances, the questions or answers may deviate from the set format.

For this research study, a semi-structured interview was conducted with: the Deputy Director of Examinations, and unstructured interviews with a few selected academic staff (who are examiners and some of whom are also internal moderators). The interviews were conducted to gain insight into the examination process, and regarding what the EPPP entails.

Questionnaires are a form of interviewing, where respondents are asked the same questions with the same options in answering (Hofstee, 2006). Although questionnaires are limited in depth in that they do not allow the researcher to probe the answers of respondents, they do, however, offer confidentiality and anonimity to the respondents, if name of responded is not required (Hofstee, 2006). The confidentiality allows for the respondents to answer openly without the feeling of being watched and judged. Furthermore, questionnaires are easier to analyze as they results could be turned into quantitative results, further, questionnaires allow for more respondents than interviews do (Hofstee, 2006).

The questionnaires were distributed to randomly selected examiners (some of whom were also internal moderators) to elicit information about their practices and about the ICT resources they use to process, store and transmit the examination papers when preparing them.

A **document review** was conducted, with the use of a qualitative content analysis for the analysis of the documentary source. Documentation is one of the multiple case study data sources, as identified by Yin (2003). A **qualitative content analysis** is a form of content analysis used for text interpretation to provide perspective about the text (Krippendorff, 2004). According to Anderson (1998), “content analysis is applied to the analysis of data in documents and refers to the systematic description of the contents of documents”.

A qualitative content analysis of the relevant documentation specific to the EPPP was conducted. Such documentation was the examination process policy and documented procedures at the NMMU. The use of qualitative content analysis assisted in the interpretation of the contents of the examination process policy and documented procedures in order to understand and bring meaning to the contents of the documents. This assisted the researcher in gaining insight into what the examination process is expected to be, in particular the EPPP, especially pertaining to the security of examination papers and what role players are expected to do.

Observation entails observing a group in its natural setting (Hofstee, 2006). Observation is ‘seeing first hand how people act in a specific setting and what the setting comprises’ (Henning, 2004) This may include interviewing the group to get a clear understanding of what they are doing.

For this research study, the researcher spent some time in the Examinations Office, in order to observe the general security of the environment and how the examination papers are handled in the Examinations Office. Furthermore, it was to observe the examiners when they brought in their examinations papers, to establish if they followed what the documented policy stated regarding the submission of examinations papers. The researcher went as far as asking the examiners if they were aware of the examinations policy and procedures and the contents thereof.

Argumentation is about establishing the benefits of a claim through considering evidence that supports it and the alternatives that may provide a more comprehensive understanding (Lapakko, 2009).

From the literature and the security concerns identified from data collected, key concepts pertaining to securing an information environment were identified, thereafter, argued towards a model that will assist in managing and improving the security of the EPPP.

Modelling Techniques were used to develop the model. 'A model captures the essential aspects of a system or process, while it ignores the nonessential aspects. It may be used to evaluate existing systems or processes' (Olivier, 2004).

For the purpose of this research study, the model will concentrate on the security of information (examination papers) during the EPPP. By creating a platform for greater awareness and understanding of relevant information security issues, as well as suitable controls; the model will be able to assist in managing and improving the security of the EPPP, thereby ensuring that examination papers are adequately and appropriately protected. The proposed model, as well as the methodology followed to develop the model is discussed in Chapter 5.

Elite/expert Interview is the use of relevant qualified people (elites/experts) to evaluate how well the solution contributes to solving the identified problem (Cooper & Schindler, 2003).

For this research study, elites in the information security domain and the HE examinations domain were used to evaluate the proposed model; to measure how well the proposed model supports a solution to the identified problem as stated in the Problem Statement (Section 1.5). The elites used were identified as relevant people who may have a significant contribution to make in the evaluation of the model. The elites were deemed relevant as they are authoritative in the roles they fulfil, and have the relevant experience in the subject matter. Two groups of participants were used as elites. One group is the information security elites, who are involved in information security research and have each published a number of journal and conference papers. Furthermore, the information security elites are academics, who have been involved in the EPPP for a number of years both as examiners and as moderators. The other group is the examinations elites, who are examinations senior management staff involved in the administration of examinations, as well as setting up policies and procedures at a particular HEI. A further discussion on the elite interview is found in Chapter 6)

Table 1.1 presents an overview of why and how the research methods were utilized in this research study, in order to satisfy the research objectives.

Table 1.1 Overview of Research Objective and the Associated Research Methods

WHAT: OBJECTIVES	WHY	HOW: RESEARCH METHODS
Proposing a model for managing and improving security and for the secure use of ICT during the Examination Paper Preparation Process at a higher education institution.	• To argue towards a solution. • To develop a model which will manage and improve the security of the EPPP. • To evaluate the model.	• Argumentation. • Modelling techniques for developing the model. • Elite interview.
To determine the current security state of the Examination Paper Preparation Process at a particular higher education institution, including identifying policies and procedures relevant to the process.	• To gain an understanding of the EPPP from the perspective of the role players. • To find out what is currently documented regarding the EPPP. • To find out to what extent security is addressed in the documentation. • To identify certain examiners' practices that could compromise the security of the examination papers.	• Observation. • Interviews. • Document Review (Qualitative Content Analysis). • Questionnaires.

WHAT: OBJECTIVES	WHY	HOW: RESEARCH METHODS
To identify relevant information security aspects and applicable information security principles from existing information security best practice frameworks and standards that need to be considered, to contribute towards a secure Examination Paper Preparation Process at a higher education institution.	• To understand what needs to be addressed and be in place, in order to ensure a secure environment. • To identify information security aspects relevant to the EPPP. • To identify information security principles that may be applicable to the EPPP.	• Literature review.
To integrate the identified information security aspects and information security principles, in order to contribute towards the development of a model for managing and improving the security of the Examination Paper Preparation Process at a higher education institution.	• To understand the organization of information security, in order to be able to coordinate and manage the information security aspects and information security principles.	• Literature review.

The next section discusses the delineation of this research study.

1.8 Delineation

This research study focuses on the EPPP, which relates to the setting, storing and transmitting of the examination papers by the examiners, internal moderators, HODs, and examination officers at a Higher Education Institution. For the purpose of this study, external examiners and external moderators are excluded, as they fall beyond the scope of the study. Although the proposed output of the study could be generalized to other similar environments, it focuses exclusively on proposing a model for improving security of the EPPP at the Nelson Mandela Metropolitan University (NMMU).

1.9 Ethical Considerations

Although this research study involved engaging with NMMU staff members for information, no personal identifiable information was required or recorded. Staff members participated anonymously of their own accord. All participants were over the age of 18 years. Only information relating to the examination process and the EPPP was required.

1.10 Dissertation Chapter Overview

This research study comprises the 7 chapters as discussed below.

Chapter 1: Introduction

This chapter is the introductory chapter. It provides an overview of the research study along with the problem statement, research questions, research objectives and methods used, including the delineation and ethical consideration sections.

Chapter 2: Information Security Management

This chapter explores literature on information security and the management thereof, through the implementation of an information security management system. The chapter further explores an ISMS as an aid for maintaining a secure information environment. In addition, the chapter identifies and explores various information security aspects that need addressing in order for any information security effort to be successful.

Chapter 3: Examination Paper Preparation Process.

The chapter discusses the examinations at a higher education institution and their purpose. The examination process is discussed in detail, focusing on the EPPP. It models the EPPP at NMMU and discusses what it entails. In addition, the chapter deliberates on the importance of ensuring that the process is secure, by assessing the process, and the importance of following a structured methodology when assessing. The chapter further discusses the suitability of the McCumber Cube for assessing the risks pertaining to the EPPP.

Chapter 4: Information Security Risks Associated with the Examination Paper Preparation Process

This chapter utilizes the methods identified and discussed in Chapter 1 to assess the risks to the EPPP. The chapter produces a list of risks, information security requirements, as well as security controls to mitigate the identified risks and to satisfy the information security requirements as outputs.

Chapter 5: Information Security Assurance Model (ISAM) for an Examination Paper Preparation Process

In this chapter the proposed model for managing and improving the security of the EPPP is constructed.

Chapter 6: ISAM Evaluation Process, Results and Analysis

This chapter presents the process followed to validate the Information Security Assurance Model (ISAM). The ISAM is the proposed model that aims to manage and improve the security of the EPPP. Expert reviewers were used to evaluate the model.

Chapter 7: Conclusion

This chapter concludes the research study and summarizes the findings. It also gives provision for future research opportunities.

1.11 Academic Publication

A peer-reviewed paper titled: *Information Security Assurance Model (ISAM) for an Examination Paper Preparation Process*, was published and presented at the ISSA 2014 conference in August 2014.

The ISSA (Information Security South Africa) conference is an international conference that uses a double blind peer-review process to review papers, to ensure the quality of submission before acceptance. The review committee consists of both local and international subject matter experts in the field of information security. Papers are reviewed and rated on a 10 point system, 1 being poor and 10 being excellent.

1.12 Conclusion

As is the case in many organizations, ICT has become prominent in HEI. ICT is being relied upon for the operations of institutions, and academic staff is embracing ICT, not only for academic purposes, but also for their administrative purposes. Examiners use ICT for preparing examination papers, as ICT provides the convenience of them being able to prepare the papers not only in the office, but remotely as well. ICT has provided the means of being able to store examination papers in mobile devices for ease of transportation. Emails have become a convenient way for examiners to disseminate the papers amongst each other when collaborating on their setting. However, if not used responsibly and securely ICT can expose the examination papers to risks, as ICT comes with its own range of risks that need to be considered and addressed. Examiners need to be made aware of such risks, to ensure that they are equipped in dealing with the risks.

The Examinations Office, although it is responsible for ensuring that there is an efficient, effective examination process that safeguards and maintains the academic integrity of the examinations, is also responsible for safeguarding a process that will ensure that risks pertaining to the EPPP are controlled and managed. This will ensure that the EPPP is secure and that examination papers are properly and appropriately protected. A risk management process is very important as it plays a vital role in achieving a secure information environment, in order to protect information assets. Therefore, a system that ensures that risks are controlled and managed appropriately is vital for securing an information environment.

Having provided an overview of the research study, by providing the background and the description of the problem area and problem description, this chapter leads to the next chapter. The next chapter explores information security for the protection of valuable information assets. The chapter progresses to the management of information security through the implementation of an ISMS. In addition, it highlights some of the essential information security aspects that need to be considered in the ISMS.

Chapter 2

INFORMATION SECURITY MANAGEMENT

2.1 Introduction

The previous chapter introduced the reader to the problem domain and the objectives of this research study. The research methodology was also discussed.

This chapter will discuss information security and the management thereof, through the implementation of an ISMS. It highlights the broad and diverse nature of information security owing to the various information security aspects that need to be considered and managed. These information security aspects need to be taken into consideration in order for information security to be effective in providing the level of protection required. In addition, the chapter will discuss the benefits of incorporating information security principles, for the effective implementation of an ISMS.

The chapter will proceed with a brief background regarding the prominence of information within an organization and the use of ICT for its use, storage and dissemination (Section 2.2). This is followed by a discussion of the importance of information security for ensuring that valuable information remains secure at all times (Section 2.3). Next, Section 2.4 discusses information security aspects which need to be considered and managed in order for information security to be effective. Following this is a discussion on information security principles as a means to aid and focus an information security effort within an organization (Section 2.5). Thereafter, Section 2.6 deliberates on the management of information security by means of an ISMS. Section 2.7 concludes the chapter.

2.2 Background

We now live in the “digital age”, where the use of electronic systems for the operations of organizations is already more prominent (Galliers & Leidner, 2003) Organizations are becoming increasingly reliant on information and communication technology (ICT) for the processing, storage and transmission of their information (Reddy, Srinivasu, Rikkula, & Rao, 2009). Computer systems and various electronic devices, such as external hard drives, Universal Serial Bus (USB) flash drives, and mobile devices, such as tablet PCs, are being used to store information and to allow information to be transported to other remote locations. Electronic methods, such as emails and on-line storage (i.e. Dropbox, Google apps, amongst others) are being used to transmit and distribute or make available documents amongst employees in an organization and beyond. However, the use of ICT, along with the Internet, has also increased the incidents of information abuse or misuse, as people are now able to access information remotely where detection can go unnoticed, as well as to remove valuable information, using mobile storage devices (Dhillon & Backhouse, 2000). Furthermore, the use of ICT and the Internet has increased and introduced a new range of threats and vulnerabilities facing information, thus putting the information at an even greater risk (Whitman, 2004). Previously, the most likely threat to information was theft, when physical entry was required to where the information was kept, as well as from forces of nature, such as floods or fire. More recently, threats could be from an even wider range of sources, such as viruses, hackers or technical failure, to name a few, all relying on the Internet and other networks to gain access to the information remotely, or to be the source of information being corrupted. When dealing with the risk, many researchers suggest managing the risks through the implementation of a proper and comprehensive information security management system (ISMS) (Eloff & Eloff, 2003; Pavlov & Karakaneva, 2011). An ISMS is “that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security” (ISO/IEC 27001, 2005). An ISMS needs to pay attention to the human factor in the organization, and the role that the human factor plays in protecting information effectively. The reason for this is that it is people who handle and work with the information of an organization on a daily basis, and these people often do so negligently and in an insecure manner. This has led to the people being labeled as the weakest link when it comes to any efforts at protecting the information assets of an organization (Posey, Roberts, & Courtney, 2011). Therefore, it is essential that this weakest link be appropriately addressed in order to ensure that information is properly protected (Albrechtsen, 2007; Sasse, Brostoff, & Weirich, 2001).

In the business world today, the Internet has become the ultimate platform for the flow of and access to information. Information has become an increasingly important feature in most organizations and new technologies have become available to facilitate its use and dissemination. This has led to the expansion of ICT (Todd, 2007). According to the National Institute of Standards and Technology (NIST), ICT is regarded as any equipment or interconnected systems, including computers and mobile devices, which are used in the processing, storage and transmission of information (NIST SP800-64, 2008). The connectivity of computers has led to the ability of workers to access and share information more easily, allowing organizations to be more efficient, effective and responsive (Dhillon & Backhouse, 2000). According to Todd (2007), these new developments in ICT have led to an increasingly mobile workforce, where employees are able to work from remote locations by using various mobile devices (such as laptops and tablets) and mobile storage devices (e.g. flash drives and external hard drives). In addition to the ICT capabilities, the Internet has also enabled new forms of human interactions. The employees can now communicate quicker by less expensive means, and can collaborate on projects through instant messaging, emails, or through the use of on-line storage, all enabled by the Internet. Although ICT and the Internet have made it convenient for employees to perform their duties, their use has exposed the valuable information of organizations to a wide range of threats (Alwi & Fan, 2010).

With the growing value of information as a business asset, and organizations increasingly relying on ICT for the processing, storage and transmission of its valuable information, the protection of information has become necessary (Hong, Chi, Chao, & Tang, 2003). According to ISO 27002 (2005), information is an asset that can exist in many forms (printed or written on paper; stored electronically; transmitted by post, hand-delivered or electronically-delivered). The NSTISSI 4011 (1994) further states that information can exist in one of three basic states: processed, stored or transmitted. Whatever the form or state, the information needs to be protected suitably from a number of threats. Threats are potential causes of an unwanted incident, which may result in harm to a system or organization (ISO 27002, 2005). Therefore, it is crucial that these threats are known and that the information assets are suitably protected from them. This protection of information from a wide range of threats is known as information security.

2.3 Information Security

Information security is the protection of information and the systems and hardware that use, store and transmit that information (Whitman & Mattord, 2003). Information can be protected by preserving its confidentiality, integrity and availability (CIA), which are the basic attributes of information (McCumber, 2005). This means ensuring that information is accessible only to authorized individuals (confidentiality); that information is not exposed to corruption, damage or destruction (integrity); and that authorized users can access information without interference or obstruction (availability) (Whitman & Mattord, 2008). Therefore, information and the various systems and technologies that it uses need to be protected from the potential threats which may pose a risk to the security of the valuable information assets of an organization.

Information security is about managing the risks to information assets. Managing risks involves the identification, the analysis, the mitigation and/or documentation of risks (Whitman & Mattord, 2008). According to the Information Organization of Standardization (ISO), information security risk is the potential that a given threat will exploit the vulnerabilities of information assets and thereby cause harm to the organization (ISO/IEC 27005, 2008). A threat is described in the ISO/IEC 27001 (2005) as "potential cause of an unwanted incident, which may result in harm to a system or organization". It is further described in the FIPS PUB 200 (2006) as "potential for a threat-source to successfully exploit a vulnerability". Threats could be categorised as natural threats or human threats, and the latter further classified as deliberate or intentional (NIST SP 800-30, 2002; Von Solms & Von Solms, 2009; ISO/IEC 27005, 2008). These threats come from a wide spectrum of threat sources and should be identified and documented (NIST SP 800-30, 2002). Vulnerabilities are weaknesses of an asset or group of assets that can be exploited by one or more threats (ISO/IEC 27002, 2005). These could be system, network or process weaknesses. According to ISO/IEC 27005 (2011), vulnerabilities could be identified by using the following methods: interviews with users, questionnaires, physical inspection and document analysis. For information security to be effective, the threats and vulnerabilities that could compromise the security of the information assets of the organization should be known and understood. Knowing and understanding the threats and vulnerabilities will ensure that they are dealt with appropriately and effectively. This could be achieved by assessing the risks.

According to the NIST (2011), the purpose of assessing risks is:

- To identify critical assets, potential threats to the organization, as well as the vulnerabilities that could be exploited by the threats, resulting in the security of the information assets of an organization being compromised.
- To determine the consequences to the organization that may occur (impact or harm), should the potential threats exploit the vulnerabilities.
- To determine the likelihood of occurrence of the consequences.

The results of the assessment will be the determination of the risks, which is the sum of the magnitude of potential consequences and the likelihood of the consequences occurring (Gerber & Von Solms, 2005). Thus, risks are the cause of threats taking advantage of known or unknown vulnerabilities. Once the risks are determined, the decision-makers will be able to determine appropriate courses of action to deal with those risks appropriately. An example of the risk could be a hacker (threat-source), hacking (threat) a weak password (vulnerability), resulting in the hacker gaining access to the confidential information (asset) of the organization (such as the personal information of customers), as a result, damaging the reputation of that organization (impact). The reputation may be damaged, and customers may lose confidence in the organization, owing to the failure of the organization in providing adequate protection for their personal information. This could result in customers not wanting to do business with the organization, leading to the loss of business for that organization. Therefore, it is essential that organizations address the identified risks appropriately and effectively, for the continuity of the organizations. This could be achieved by ensuring that the assessment be part of a bigger picture for creating and maintaining a secure environment that will protect the information assets of the organization appropriately and effectively.

To provide appropriate and effective protection, various aspects need to be considered, controlled and managed, rendering information security that is broad and diverse (von Solms, 2001).

2.4 Information Security Aspects

According to von Solms (2001), information security needs to be addressed in a holistic and comprehensive manner, taking into account all the relevant aspects. These aspects, also identified as facets or components by other researchers, include: the organizational structure; policy; best practices; risk assessment; awareness, education, and training; the human factor; as well as compliance, amongst others (Von Solms, 2001; Von Solms & Von Solms, 2004; Killmeyer, 2006). For the purpose of this research study, these shall be refered to as aspects. Some of these aspects are also identified as security controls or best practices by some information security standards and best practice frameworks. Each of these aspects is discussed in detail in the following sections.

2.4.1 Organizational Structure

Organizational structure deals with “the way information security is organized and structured in an organization” (Von Solms B., 2001). For information security efforts to be successful, information security has to be managed and coordinated properly within the organization. According to the International Organization for Standardization, a management framework needs to be established to initiate and control the implementation of information security (ISO/IEC 27002, 2005). The management framework should set clear direction, with the commitment of top management and its support of the information security implementation. An information security team needs to be set, and clear roles and responsibilities need to be assigned. If there is a need, information security specialists should be enlisted, and contact with relevant groups should be made, in order to keep abreast with relevant new information as well as with standards and best practices (ISO/IEC 27002, 2005; NIST SP 800-53 Rev 3, 2009).

The management framework needs to identify information security goals and requirements, which will be translated into the information security policy. The policy needs to be reviewed and approved by top management. The top management is also responsible for establishing a risk management strategy, and for ensuring that all necessary resources are available for the successful implementation of information security. Top management is also responsible for ensuring that there are plans and programs in place for the awareness, education and training of all relevant persons who handle the information assets of the organization (ISO/IEC 27002, 2005).

2.4.2 Information Security Policy

Information security policy is a direction-giving document for information security within an organization, providing management direction and support for information security (Hone & Eloff, 2002). It should therefore, state the commitment of management to information security, in order for the rest of the organization to take information security efforts serious. The policy is a general guide from management regarding the means of protecting the information assets of the organizations. It is a document based on the need for information security and the role that it has in protecting the information assets of the organizations from identified threats (Schweitzer, 1982). According to Killmeyer (2006), it is a necessary foundation of an information security programme, and it creates a guideline for a consistent and effective implementation of security controls.

The policy is further used as a communication mechanism between management and information users to communicate various information security issues and concerns that need addressing (Killmeyer, 2006; Hone & Eloff, 2002). It defines the roles and responsibilities of the information users with regard to information security. It further communicates to users the appropriate way of handling the information and ICT systems and resources of the organization. In addition, the policy provides users with knowledge on means of protecting the valuable information assets effectively (Killmeyer, 2006). The policy thus guides the actions of users when handling information assets, informing them of acceptable and unacceptable behavior while handling the information assets of the organization. Subsequently, it inform users of the penalties of not following the policy (Hone & Eloff, 2002).

The users should therefore be able to apply the defined security practices as in accordance with the established policy (Doherty, Anastasakis & Fulford, 2009). This will assist users in their responsibility of protecting the valuable assets of the organization, as they are responsible and are held accountable for the security of the information assets they handle.

However, quite often the users are unaware or ignorant of the policy in existence, which compromises the effectiveness of the policy (Hone & Eloff, 2002). For the policy to be effective in providing guidance, it is imperative that the policy be communicated properly to all relevant parties (Hone & Eloff, 2002). The users need to be aware of the policy, as well as to understand it. It is thus essential that the policy be simple and easy to understand, so as not to be misinterpreted by the users (Forte, 2000). In addition, users should be able to identify with the policy and to see clearly what is expected from them as far as information security is concerned (Hone & Eloff, 2002).

According to the guidance of international best practice frameworks (ISO/IEC 27002, 2013; IT Governance Institute, 2007), in order for the policy to be effective, it should:

- state the commitment of management to information security, in order for information users to understand how serious management is about information security;
- define clearly the roles and responsibilities, so that information users know what they must do and what is expected of them;

- communicate to the intended audience in relevant forms, so that they will be aware of the policy;
- be accessible and understandable to its intended readers; and
- state the consequences of policy violation, in order that the information users understand how important the policy contents are.

In conclusion, the policy should be able to foster secure practices within users while performing their daily operations. Furthermore, the policy needs to be enforced, and users need to adhere to it, in order to prevent the security of the information assets from being compromised. Best practices stress the importance of a policy.

2.4.3 Best Practices

Best practices, also referred to as good practices, are "proven activities or processes that have been successfully used by multiple organizations" (ISACA, 2012). These are security efforts that are amongst the best in the industry and seek to provide protection for information assets (Whitman & Mattord, 2008).They are tried and tested practices that, if followed, may help to address most information security risks, and may assist in ensuring that all information security bases are covered (Von Solms, 2001). Best practices usually document the knowledge and experiences of a group of people, as far as information security is concerned (Von Solms & Von Solms, 2009). The best practices describe a set of detailed issues, which should be addressed to achieve specific information security objectives (Eloff & Von Solms, 2000).

The best practices are reference frameworks to help guide the development and implementation of the ISMS. These assist in ensuring that all the information security aspects are addressed and covered in the ISMS. These can be followed and adapted to secure an information environment (Stefanek, 2002). They also assist in: formulating actions to information security requirements; ensuring that the security risks are managed effectively; ensuring compliances with laws and regulations; and in giving a process framework for the implementation and management of security controls (Pavlov & Karakaneva, 2011).

Recognized best practice frameworks include COBIT (IT Governance Institute, 2000), the NIST Special Publications (NIST, 1996) and the ISO 27002 (ISO/IEC 27002, 2013). Each of these best practice frameworks will be discussed individually.

- **COBIT** (Control Objectives for Information and Related Technology) is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risk (ISACA, 2012). As information and the technology that supports it represent the valuable assets of an organization, there is a need to understand and manage the associated risks. COBIT recognizes that effective management of information and related IT is critically important to the success and survival of organizations (Lainhart IV, 2000). It addresses IT governance and refers to information security, amongst many other issues (Von Solms, 2005). It assists in managing and controlling IT risks and vulnerabilities effectively. COBIT focuses on what is required to achieve adequate management and control of IT.
- **NIST** (National Institute of Standards and Technology) is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems. The **NIST Special Publications** are developed and issued as recommendations and guidance documents for security efforts (NIST SP 800-39, 2011). The NIST Special Publications (800 series) was established in 1990 to provide for IT security, in order to report on research, guidelines and outreach efforts in computer security (NIST, 2007). These Special Publications cover information security topics, such as the following: managing information security risk; recommended security controls for federal information systems and organizations; generally accepted principles and practices for securing information technology systems; and security and privacy controls for federal information systems and organizations amongst others. The Special Publications are developed to produce an information security framework, as well as for a process for selecting and

specifying safeguards and security controls for federal information systems (NIST SP 800-53, 2009).

- **ISO 27002** (International Organization for Standardization) is a code of practice for information security management (ISM) and may serve as a practical guideline for developing organizational security standards and effective security management practices (ISO/IEC 27002, 2013). ISO 27002 contains 14 security control clauses, which collectively consist of 35 main security categories in total. Each of the security control clauses is dedicated to a specific aspect of information security, which needs to be addressed to ensure a secure information environment (Von Solms & Von Solms, 2009). Each main security category contains a control objective stating what is to be achieved and one or more controls that can be implemented to achieve the control objective (ISO/IEC 27002, 2013).

These best practice frameworks can assist in ensuring that all identified information security risks are managed in an effective and appropriate way. Before risks can be managed, they need to be identified and assessed.

2.4.4 Risk Assessment

Risk assessment is essential for the identification and evaluation of risks pertaining to a particular environment, or the use of ICT systems for the processing, storage and transmission of valuable information. The results of the risk assessment can thereafter help to guide and determine appropriate actions and suitable security controls for the mitigation and management of the risks (NIST SP 800-30, 2002; ISO/IEC 27002, 2005). Implementing information security controls based on identified risks pertaining to the particular environment is a cost-effective way, as only the required controls that meet the needs of the organization will be implemented (NIST SP 800-30 , 2002). Risk assessment helps to identify: the most valuable assets that require the most protection; the threats that could cause potential loss or damage to the organization; as well as potential vulnerabilities that exist, that could be exploited by the threats resulting in risk (ISO/IEC 27005, 2011).

According to ISO27005 (2011), the process of assessing risks includes: risk identification, risk analysis, and risk evaluation.

- **Risk identification** entails identifying: the information assets that require protection; the applicable threats pertaining to the information environment and organization; and the vulnerabilities that exist or could exist, which could be exploited by the identified threats (Gerber & Von Solms, 2005; ISO/IEC 27005, 2011). It further includes identifying existing security controls, in order to determine their effectiveness in dealing with the identified risks, so that other security controls can be identified and selected, if need be (ISO/IEC 27005, 2011). Once the information assets of the organization that require protection, as well as the potential threats and vulnerabilities, are listed along with the existing security controls, the level of risk can be determined through risk analysis.

- **Risk analysis** is about "obtaining the general indication of the level of risks and revealing the major risks" (ISO/IEC 27005, 2011). It entails quantifying the level of risk, by taking into account the magnitude of the potential consequences to the organization, should a threat succeed in exploiting a vulnerability, as well as the likelihood of the consequences occurring (ISO/IEC 27005, 2011). The risk can be measured qualitatively or quantitatively. Measuring risk qualitatively makes use of descriptive scales (such as low, medium or high values) to describe the level of risks, while measuring risks quantitatively uses numeric values (such as monetary values) to relate the costs of obtaining and/or maintaining the asset should it be compromised (Gerber & Von Solms, 2005).

  The analysis could be accomplished by creating incident scenarios, which include the threats and vulnerabilities, and the affected assets, as well as the consequences to the assets and/or organization (ISO/IEC 27005, 2011). For example, a hacker cracks a weak password of the financial manager of an organization, resulting in the hacker having access to major business accounts and being able to transfer large amounts of money. The extent of the consequence to the organization could be huge; the organization could loose huge amounts of money, rendering it unable to continue business; and the likelihood of this happening could be increased owing to the weak password. Although the security control is there (the password), however, it is ineffective owing to its weakness, because it could be easily cracked. The risk can thus be measured qualitatively as **high** risk owing to the high magnitude of damage to the organization, should the accounts be accessed by an unauthorized person through the weak password. Or, the risk could be measured quantitatively, by producing the monetary value of the financial loss to the organization. Following the risk analysis is the risk evaluation.

- **Risk evaluation**. is calculating the risk based on the values assigned during risk estimation, for probability and impact of harm to the information assets of the organization (Gerber & Von Solms, 2005).

The results will assist in determining how the risks should be managed. The results will then help to identify, select and implement the needed security controls for the mitigation of those risks, thereby protecting the valuable information assets of the organization. When determining risks, the human factor has to be considered, as it's the users who handle the information assets on a daily basis.

2.4.5 Human Factor

Humans, or information users, play a vital role in maintaining a secure information environment, and in ensuring that information assets are protected at all times. In the past the protection of information assets was seen as a technical issue, where technology was the solution. However, recently it has come to the attention of many information security professionals that technology alone does not produce a secure information environment, because the securing of information is not solely a technical issue, but a human issue as well (Parsons, McCormac, Butavicius & Ferguson, 2010). Computer systems which process, store and transmit the information assets are operated by people, and it is the very same people who work with and handle the information assets of the organization on a daily basis. Owing to the interaction of people with information and information technologies, which is often detrimental to the security of information, information security is no longer just a technical issue, but a human issue as well (Parsons, McCormac, Butavicius & Ferguson, 2010). No matter how well a security system is developed and implemented, it depends on people in order to be effective. Therefore, as Ashenden (2008) states, the management of information security depends on technology, processes and people.

As humans will always be part of the organization, working with information, their behavior towards handling information securely needs to be considered at all times and addressed as an important part of the management of information security (Colwill, 2010). Studies have shown that more than half of identified information security breaches are caused by human error (Gonzalez & Sawicka, 2002). These security breaches could be intentional, or due to negligence or ignorance of security measures, as well as being due to lack of information security knowledge (Vroom & Von Solms, 2004). In addition, the perceived absence of risk may also cause employees not to comply with security measures, and as a result, causing security breaches.

It is therefore the responsibility of the organization to ensure that every information user in the organization is aware of: information security risks pertaining to the organization; the various security measures in place for the mitigation of those information security risks; as well as knowing what is expected of them regarding information security, in order for the organization to operate in a secure information environment and for the information assets of the organization to be protected. For these reasons, it is essential that the human factor be addressed properly and be dealt with appropriately within the organization.

The human factor involves addressing information security issues before a user is employed and granted access to information and the ICT systems; during the employment of the user; while working with the information and ICT systems; as well as after the user is no longer employed (ISO/IEC 27002, 2013). Before employing users the organization needs to ensure that the persons being employed are suitable for the role, and that the persons understand their roles and responsibilities. This also involves ensuring that the persons know what is expected of them regarding information security

(ISO/IEC 27002, 2013). Thereafter, during employment, the persons need to be made aware of the information security risks pertaining to the organization, as well as the security controls that are in place for the mitigation of the risks. Furthermore, the persons need to be made aware of the information security policy, which dictates appropriate and inappropriate behaviour, amongst other information security issues (NIST SP 800-53 Rev 3, 2009). In addition, the persons need to be equipped with knowledge and skills to perform their duties securely. The organization also needs to ensure that adequate levels of awareness of security matters are provided, as well as to ensure that the users are educated in order to be knowledgeable. Furthermore, the users need to be trained in the correct use of security controls and ICT systems that are used for the processing, storage and transmission of the information. Lastly, after employment has ended, the organization must ensure that any access rights to information and the ICT systems are revoked, and that any equipment of the organisation is returned (ISO/IEC 27002, 2013). Once these concerns of the human issues have been properly addressed and appropriately dealt with, the organization can feel confident in that its information users can participate actively in the effective protection of its information assets (Von Solms & Von Solms, 2004). Within the discussion of the human factor, the awareness, education and training aspect is emphasized as vital for ensuring that the users know what they are required to do, and understand what is expected of them regarding information security.

2.4.6 Awareness, Education and Training

Awareness, education and training, are means through which an organization can change the behaviour of information users in order to achieve high levels of information security and compliance with security controls. Awareness, education and training are fundamental aspects of information security, because users need not only to be made aware of potential risks to information, but also need to be taught the correct way of using the appropriate controls in order to contribute to the effective protection of the information.

Awareness, education and training are about ensuring that all information users are aware of and educated regarding information security in the organization, as well as trained (ISO/IEC 27001, 2005). Awareness is about informing information users of threats and vulnerabilities that could compromise the security of information assets. Through awareness, information users are also informed of their information security responsibilities as documented in the information security policy, as well as of any other issues pertaining to the protection of information (ISO/IEC 27002, 2013). Furthermore, through awareness, proper rules and behavior for use and the handling of information and ICT systems are explained. Awareness also allows information users to be informed about proper incident reporting channels (ISO/IEC 27002, 2013; Von Solms, 2001; NIST SP 800-50, 2003).

Organizations can have the best information security programs, with the best technical security controls, as well as well-written information security policies and procedures; however, without information users being aware of those, they do not serve any purpose (Furnell & Thomson, 2009). Owing to lack of awareness, information security could be compromised by the information users. Thus, awareness is a vital aspect of any information security effort (Von Solms, 2001). Users should be made aware of the dangers of, for example, choosing weak passwords; of not changing their passwords when needed; and of sharing IDs, amongst other things. In addition, users need to be educated about the importance of security awareness, and this should incorporate behavioral awareness. Awareness should be accompanied by education and training.

Education is important in order for information users to be knowledgeable, and to know why they have to do things the way they are documented, as well as the benefits of doing things in a certain way. Training exists to help train users in the correct use of information security controls, as well as the ICT systems they use for the processing, storage and transmission of the information. Awareness, education and training are for all information users, including management and contractors. Therefore, any programmes developed for the purpose of awareness, education and training should suit the relevant target audience (ISO/IEC 27002, 2013). Along with ensuring that users are aware, educated and trained, it is important to ensure that the users comply to the information security policies.

2.4.7 Compliance

Compliance relates both to legislative compliance and information security policy compliance. It ensures that appropriate security controls are in place in order to avoid breaches of any legal form such as law, regulation or contractual obligation (ISO/IEC 27001, 2005). Certain aspects of the information that the organization handles may be subject to legal requirements as imposed by state or country. Therefore, it is essential that the organization identifies such legal requirements and ensures that it complies with those that have been identified. Furthermore, the organization needs to "ensure that security activities are executed in compliance with established information security policy. As well as identify how to handle non-compliance" (ISO/IEC 27002, 2013). Compliance also involves the monitoring and evaluating of security controls to ensure continuous compliance with the security requirements of the organization as changes in the environment take place, to ensure that the security still addresses the change. For this study, compliance concentrates on policy and security controls.

Therefore, to provide appropriate and effective protection, all these information security aspects need to be considered and incorporated into an information security framework. To be able to address and incorporate these aspects in a framework, information security principles need to be considered.

2.5 Information Security Principles

Information security principles are guiding statements meant to address security concerns that could hamper the organization. Principles provide a common framework to connect and maintain information security within the business functions of the organization, by ensuring that information security is introduced and integrated into the information architecture of the organization (Jochem, et al., 2006).

Principles determine the course of action by providing an approach for planning and setting up an information security plan (Jochem, et al., 2006). They form a foundation for any information security solution, which will provide the best possible and relevant solution to address the security concerns of an organization in a cost-effective manner. According to the Information Security Forum (ISF, 2010), principles help to focus an information security effort by ensuring that:

- the focus is on the business and that information security is integrated into the business functions;
- information security accountability and responsibility within the organization is addressed and that there are consequences to unfavorable actions of users;
- there is proportionality of security controls, i.e. security controls are proportionate to the risks facing the organization and the impact to the organization;
- information security is multidisciplinary, i.e. it takes into consideration the viewpoint of all relevant departments and interested parties; and that all parties are involved in the decision-making;
- there is awareness within the organization, i.e. ensuring that all parties are informed of threats to the information of the organisation, as well as means to counter the risks caused by those threats. Parties should be made to understand the importance of information security in order to promote a culture of security within the organization; and
- there is a periodic assessment of risks in order to account for new and changing threats to information This will promote continual improvement to information security.

As Furnell, Gennatou and Dowland (2002) have stated, achieving the appropriate levels of security depends on a multi-faceted system, which covers various relevant aspects and is informed by various information security principles, in order to ensure that the information security efforts address all relevant information security issues and concerns of an organization. A multi-faceted system is a means by which management can prove that due care and due diligence were performed during decision-making, as far as information security is concerned. Through the multi-faceted system, management can prove that necessary steps were taken in order to provide adequate protection for information assets, such as personal information, which is a requirement by law. Management could also be confident that necessary steps were taken in managing risks to the information assets of the organization. For the system to be effective it requires proper and comprehensive management, which could assist in ensuring that any information security efforts are successful, as stipulated in the organizational structure aspect. Information security management can assist in ensuring that nothing is overlooked and that all aspects are taken into consideration. To help ensure a focused information security effort that addresses the security concerns of an organization, relevant activities need to be considered and addressed. To assist in the identification and co-ordination of these activities a management system should be considered. This could be achieved through the implementation of an information security management system (ISMS), which is discussed in the next section.

2.6 Information Security Management System (ISMS)

To manage the control and protection of information assets, organizations should establish and maintain a documented ISMS (Hong, Chi, Chao, & Tang, 2003). An ISMS can be defined as *'*Coordinated activities to direct and control the preservation of confidentiality, integrity, and availability of information' (Tipton & Krause, 2008)*.* Eloff and Eloff (2003), further define an ISMS as a management system used for establishing and maintaining a secure information environment.

Thus, an ISMS can assist organizations in managing information security in a holistic manner, through a holistic approach (collective manner). According to Patterson (2003), a holistic approach to security means integrating technology, procedures and people to protect information assets effectively and efficiently. This approach provides means to ensure that all relevant information security aspects that deal with creating and maintaining a secure information environment are taken into consideration. As the ***organizational structure*** aspect suggests; for an information security effort to be successful, information security has to be managed and coordinated properly, therefore, an ISMS assists in that regard. Furthermore, International best practice standards and the advice of other researchers suggest basing an ISMS on a risk approach (ISO/IEC 27001, 2005; NIST SP 800-39, 2011; Tipton & Krause, 2008). A risk approach means identifying, selecting and implementing security controls based on identified risks pertaining to the particular environment in which the organization operates. The approach, through a risk assessment, could ascertain that the threats and vulnerabilities that could compromise the security of the information assets of the organization are known and understood, in order to deal with these appropriately and effectively.

2.6.1 Assessing Risks

Assessing risks is an integral part of managing risks of an organization and provides decision-makers with the necessary information needed to respond to identified risks (NIST SP 800-39, 2011). The process of assessing risks is crucial in managing and maintaining information security effectively (McCumber, 2005). This helps in understanding and considering the full spectrum of potential threats and vulnerabilities, which could compromise the security of the information assets of the organization. Furthermore, security requirements for the organization could be determined.

Security requirements are defined by Gerber, Von Solms and Overbeek (2001), as the amount of security needed to provide the required level of information security for the information assets of an organization. Once the security requirements are determined, the best way of meeting and satisfying these can then be discussed. According to ISO 27002 (2013), there are three main sources of security requirements:

- the assessment of risks;
- the legal, statutory, regulatory and contractual requirements that an organization has to satisfy;

- the set of principles, objectives and business requirements for information handling, processing, storing, communicating that organization has developed.

A risk assessment is a cost-effective way of managing risks, as it is based on identified risks, resulting in a fundamental justification of the selection and deployment of security controls. The security controls will thus provide the required level of information security, enabling risks to be properly managed and controlled. Risk assessment should, thus, be followed by risk management.

2.6.2 Risk Management

Risk management "refers to the planning, monitoring and controlling activities which are based on the information produced by risk assessment activities" (Gerber & Von Solms, 2005). Managing risk can be based on four basic options: risk avoidance, risk transference, risk reduction, and risk retention/ acceptance (ISO/IEC 27005, 2011).

- Risk avoidance refers to avoiding the activity or condition that gives rise to the particular risk.
- Risk transference is transferring the associated risk to other areas or parties, e.g. insurers.
- Risk reduction is applying appropriate security controls to reduce the risk to an acceptable level.
- Risk retention/ acceptance is acknowledging and accepting risk objectively, provided that the risk satisfies the criteria of the organization for risk acceptance (ISO/IEC 27005, 2011; Whitman & Mattord, 2008; Von Solms & Von Solms, 2009).

For those risks where applying security controls is the decision, the appropriate and justified controls should be selected and implemented to meet the requirements identified through risk assessment. Some of the security controls are referred to as best practices. Security controls can be selected from ***best practice*** standards such as the

ISO 27002, the NIST special publications and/or Control Objectives for Information and Related Technology (COBIT), or from other control frameworks.

The security controls are classified into three categories: the management, operational and technical controls. For the controls to provide adequate protection, it is recommended that a combination of controls within the three categories be selected, in order to provide the required level of security for the information assets of an organization (NIST SP 800-30 , 2002). The three categories of controls are:

- **Management controls** focus on the stipulation of information security policy, guidelines and standards. These controls set the direction and scope of the information security process and provide detailed instructions for its conduct. The controls also address the management of risk (NIST SP 800-30, 2002; Whitman & Mattord, 2008).
- **Operational controls** cover management functions and lower-level planning, such as disaster recovery. In addition, the controls cover personnel security and physical security as well as providing for the development of user education, training and awareness programmes (NIST SP 800-30 , 2002; Whitman & Mattord, 2008).
- **Technical controls** address the tactical and technical issues related to designing and implementing security in the organization. These controls address safeguards that are incorporated into computer hardware and software (e.g. access control mechanisms, and identification and authentication mechanisms) (NIST SP 800-30, 2002; Whitman & Mattord, 2008).

When the appropriate controls are identified, selected and implemented, they can ensure that information security risks are reduced to an acceptable level. The acceptable level of risk is the desired target of risk that an organization is willing to accept, based on risk acceptance criteria that an organization has developed and specified (ISO/IEC 27005, 2011). The management, operational and technical controls are therefore essential for managing identified information security risks; and for reducing the risks to the acceptable level, as well as for providing the needed protection for the information assets of an organization. However, controls need to operate effectively for them to be effective in providing the needed protection (Barnard & von Solms, 2000). Therefore, it is imperative that organizations monitor and evaluate the operations of the controls and their effectiveness in addressing the identified risks to information assets on a continual basis.

Furthermore, the effectiveness of controls depends to a large extent on appropriate levels of user ***awareness, education and training***, as well as ***compliance***. Users need to be made aware of the threats to the information assets of the organization and the various controls implemented for the mitigation of the risks posed by the threats. Furthermore, it is essential that users are educated regarding information security in order for them to be knowledgable about certain security issues pertaining to the organization (Thomson & Von Solms, 1998). In addition, users need to be trained, to be able to utilize the controls correctly, as well as in the correct use of the ICT systems used for the processing, storage and transmission of the valuable information assets of the organization. In essence, it is essential that users know and understand their roles and responsibilites regarding information security, for them not to compromise the security of the valuable information assets of the organization.

One of the single most important means of ensuring that users are aware of certain security issues and concerns, as well as knowing what is expected of them regarding information security, is through an ***information security policy***. An information security policy is an effective communication mechanism for management to inform information users of security issues, and to inform them of their roles and responsibilities, as well as to guide and dictate appropriate secure behaviour. Therefore, it is very important that users are also made aware of the information security policy (Hone & Eloff, 2002; Killmeyer, 2006).

For the information security policy to be effective and to address what is relevant, it is recommended that it be based on information security best practices (Hone & Eloff, 2002).

From the above, it is obvious that all relevant information security aspects play a very active role in the management of information security and should then be addressed prominently within the ISMS. This will help in creating and maintaining a secure information environment, an environment that protects the valuable information assets of an organization. To help structure the processes and activities of the ISMS, a Plan-Do-Check-Act (PDCA) Model can be used.

2.7 Plan-Do-Check-Act (PDCA) Model

The PDCA model is a model adopted by ISO 27001 (2005) for establishing, implementing, maintaining and reviewing an ISMS. The PDCA model is applied to structure all the ISMS processes. The model helps to govern the guidelines for risk assessment, security design and implementation, as well as security management and reassessment (ISO 27001, 2005). The PDCA model is divided into 4 phases: Plan; Do; Check and Act. Table 2.1 is a presentation of how the PDCA Model is applied to structure the processes of the ISMS and the Information Security Risk Management Process.

Table 2.1 PDCA Model Applied to the ISMS and Information Security Risk Management Process according to the ISO 27001 and ISO 27005 Standards

PDCA Model	ISMS	Information Security Risk Management Process
Plan	**Establish the ISMS** - Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with the overall policies and objectives of an organization.	Establishing the context. Risk assessment. Developing risk treatment plan. Risk acceptance.
Do	**Implement and Operate the ISMS** - Implement and operate the ISMS policy, controls, processes and procedures.	Implementation of risk treatment plan.
Check	**Monitor and Review the ISMS** - Assess and,	Continual monitoring and reviewing of risks.

	where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.	
Act	**Maintain and Improve the ISMS** - Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.	Maintain and improve the Information Security Risk Management Process.

With the PDCA model, all the activities of the ISMS can be structured in a process. These activities could include all the various information security aspects which need to be considered in order to protect an information environment.

2.8 Conclusion

This chapter explored information security and the management thereof, through the implementation of an ISMS. The chapter demonstrated the importance of an ISMS for creating and maintaining a secure information environment, which ensures that information assets are protected adequately and appropriately. The amalgamation of information security aspects, and information security principles, in order to develop a sound ISMS, was also addressed. It was also further highlighted how fundamental the human factor is. The reason for this is that an organization can have the best information security system in place; however, without the participation of the users, the system will be ineffective. In addition, the PDCA model was discussed as means of structuring the processes of the ISMS.

With this understanding, the following chapters will determine the need for applying the ISMS concept to the EPPP of a higher education institution, to aid in improving the security of the process, in order to provide adequate and appropriate protection for the examination papers. The next chapter introduces the EPPP of a particular higher education institution, illustrating what the process entails. It highlights the importance of ensuring that the process is secure, and that it preserves the CIA of examination papers, thereby establishing the need for applying the ISMS concept to improve the security of the EPPP.

Chapter 3

EXAMINATION PAPER PREPARATION PROCESS

3.1 Introduction

The previous chapter introduced information security as a means for protecting valuable information assets, as well as the management thereof through the implementation of an ISMS. The chapter described ISMS as a system that ensures that all relevant aspects of information security are taken into account, in order to create and maintain a secure information environment; ensuring appropriate and adequate protection for information assets. With this understanding, the ISMS concept will be explored and adopted for managing and improving the security of an Examination Paper Preparation Process (EPPP) of a higher education institution, in order to ensure that examination papers are appropriately and adequately protected.

This chapter will introduce and describe the EPPP in detail. The chapter models the EPPP of a particular higher education institution, in order to understand how the process is structured and what it entails. Furthermore, the chapter will elaborate on the importance of risk assessment, as well as on following a structured methodology for the assessment of risks.

This chapter will proceed by briefly discussing examinations (Section 3.2); in order to understand the importance of examinations. Following that will be a brief discussion of a typical examination process, before delving into the description and discussion of the EPPP (Section 3.3). In addition, Section 3.4 of the chapter will briefly discuss the importance of assessing the EPPP for risks, followed by information security risk assessment methodology (Section 3.5), which is recommended as a means of structuring an information security risk assessment. This will be followed by a discussion of the McCumber Cube methodology (Section 3.6), which was identified as applicable to aid in the assessment of risks pertaining to the EPPP (Section 3.7). The assessment will be discussed in Chapter 4. This chapter concludes in Section 3.8.

In the next section a brief discussion on examinations is provided.

3.2 Examinations

As stated in Chapter 1, examinations assess the knowledge of a student to give assurance that the student has sufficient understanding of that which is being assessed. Examinations are assessment methods that collect evidence of the competence of a student to demonstrate the achievement of the learning outcomes of a module.

Institutions conduct various forms of assessment, as a means of evaluating the level of knowledge the student has grasped. Assessments can be in an oral form or a written form, and can include essays, assignments and reports. These may take place as course work or time-limited written examinations (University of East London, n.d). "*Assessment* describes any processes that appraise an individual's knowledge, understanding, abilities or skills" (Quality Assurance Agency, 2006). According to the Quality Assurance Agency (2006), the purpose of the assessments include:

- Evaluating the knowledge, understanding, abilities and skills of students;
- Establishing the extent to which the students have achieved the intended learning outcomes of a module or programme; and
- Enabling the public (including employers), to know that the individual has attained an appropriate level of achievement that reflects the academic standards set by institutions.

In an attempt to achieve the assessment purposes, institutions should ensure that assessments are conducted with strictness, integrity and due care. Additionally, this should include ensuring that examination papers are protected from various threats, by ensuring that the EPPP at the institution is secure and that it maintains academic integrity. Should examination papers be accessible to unauthorized individuals before the examinations take place, this will not only undermine the integrity of the examination process in its entirety, but of the university as a whole. As a result, this may cost an institution its credibility in the industry, and furthermore, may cost the institution funding and a decrease in the number of student enrolments.

Chapter 1 pointed out the influence that the reputation of an HEI has in attracting and securing much needed funding for the institution. This is important owing to the financial constrains faced by institutions, as a result of limited financial resources. Various items were identified as having an influence in maintaining a good reputation, the EPPP being one of them. The EPPP, if not managed securely, can have an adverse impact on the reputation of the institution. Therefore, it is imperative that the institution ensures that an effectively controlled and secure EPPP be in place; an EPPP that ensures that examination papers are not accessible to unauthorized persons before the examination takes place. In order to have a secure EPPP, risks pertaining to the EPPP should be assessed and mitigated.

Before trying to identify risks pertaining to the EPPP in order to identify ways of addressing those, it is fitting that the process should be explored, in order to see how it is structured and what it entails. Understanding the EPPP will assist in ascertaining that all risks pertaining to the process are identified in order to deal with them appropriately. The following section introduces the EPPP. The section starts by describing a typical examination process before it zooms in on the actual EPPP.

3.3 The Examination Paper Preparation Process

A typical examination process encompasses various sub-processes, each in turn comprising a collection of activities. The examination process includes the preparation of the examination papers by the responsible examiners; appointing of external examiners and moderators; ensuring that the examination papers are moderated on time to ensure that the papers are of an acceptable quality and that the required outcomes are achieved; preparing timetables in a way that scheduled examination times and dates of the various subjects do not clash and that students have sufficient time between examinations for preparation; allocating examination venues; ensuring that there are enough invigilators; and ensuring that the examination papers are printed and ready on time for the examination (NMMU, 2008).

As mentioned, part of the examination process includes the EPPP. The EPPP is a process that ensures that examination papers are set and ready for the examination to take place. The process ensures that the papers are compiled, moderated and authorized on time, before the papers are taken to the Examinations Office to be duplicated and kept securely until the date of the examination. During the EPPP, a vast magnitude of confidential information is handled by multiple people. These people are the role players (internal examiners, internal moderators, Head of Departments, and examinations officers) within the process. The information can be in various forms; printed or written on paper; stored electronically, or transmitted by post; hand-delivered or by electronic means. Regardless of its form, this information can also exist in one of three basic states; processed, transmitted, and stored.

Figure 3.1 depicts the EPPP of a particular higher education institution, based on these three states (which are discussed in the following points):

- **Processing** – this constitutes the compilation of the examination papers, which goes through four stages: Setting; Moderation; Authorization; and Submission.

- **Transmission** – this illustrates the transmission of examination papers amongst the various role players within the process.

- **Storage** – this depicts the various locations where the examination papers can be found, and the types of devices in which the examination papers can be stored.

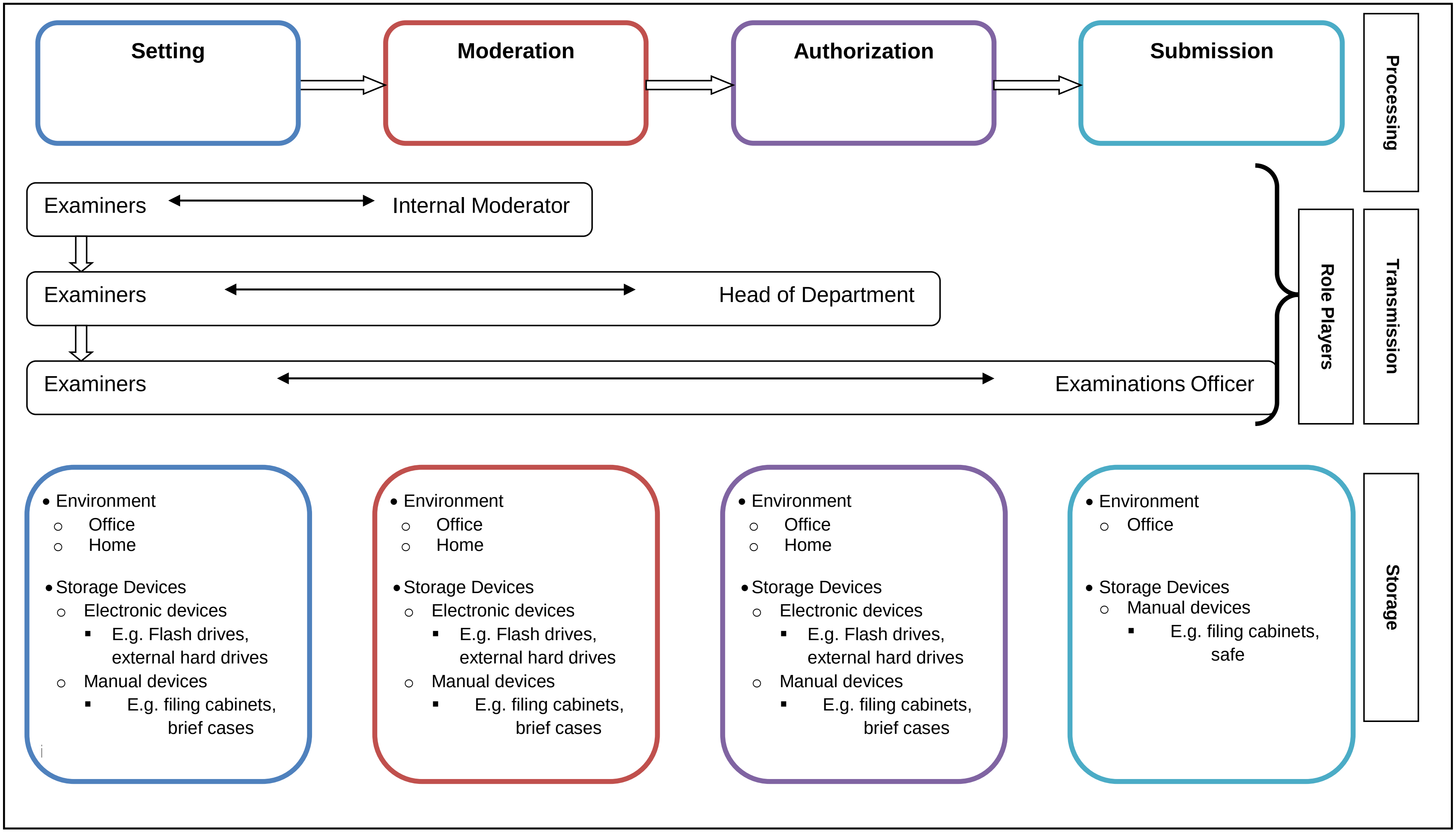


Figure 3.1 Examination Paper Preparation Process

During the EPPP, the processing of the examination papers goes through four stages (Setting; Moderation; Authorization; and Submission), as illustrated by **Processing** in Figure 3.1. During the EPPP, an examiner, or multiple examiners collaborating on the examination paper, set the paper. This could be done by drafting the questions on paper or by using ICT resources, such as a PC, to draft the question. During that time, the paper is constantly communicated and transmitted amongst the examiners.

Once the questions are completed, the paper is sent to the internal moderator to be moderated, as depicted by **Transmission** in Figure 3.1. As explained in Chapter 1, this research study will only concentrate on the internal moderation of the examination papers, as external moderation falls beyond the scope of this research study. Once the examination paper is moderated, it is sent back to the examiner, to update the paper based on the recommendations suggested by the moderator, if any. The examination paper is then sent to the HOD for authorization and is then submitted to the examinations office. For the EPPP, four role players are identified: the internal examiners, internal moderators, HODs and examination officers, as represented by the **Role Players** in Figure 3.1.

Throughout the process, the examination papers can be found in any of the various locations as presented by **Storage** in Figure 3.1. These locations refer to where role players work (office and/or home), as well as the various types of storage devices used to store the examination papers. These storage devices may include filing cabinets, desk drawers, brief cases, flash drives, and external hard drives, amongst others. To transmit the papers from one location to the next, as well as for storage, information and communication technology (ICT) has very much come to be relied upon. As ICT has infiltrated higher education institutions, with the processes of the institutions becoming increasingly reliant on ICT for the processing, storage and transmission of information, the EPPP has also started to depend to a large extent on ICT. Examination papers are mostly being set, stored and distributed through the use of modern ICT.

In a typical scenario, examiners make use of technology for the preparation of examination papers. The examination papers are stored on hard drives, network drives, in the “cloud”, or on portable storage devices (i.e. external hard drives, flash drives, or mobile devices, such as tablets). These devices make it convenient for examiners to work remotely on the examination papers. Furthermore, the use of the Internet via email allows examiners to collaborate quickly and easily on the setting of examination papers. Although ICT has made it more convenient for the examiners to prepare their examination papers, it also has its downside. As stated in Chapter 1, technology is exposed continuously to a wide range of threats, which may compromise the security of the examination papers, which may, in turn, undermine the integrity of the examination process in its entirety.

Such threats could include, amongst others:

- unauthorized persons gaining access to stored examination papers (on network drives, hard drives, mobile storage, etc);
- unauthorized persons intercepting examination papers being transmitted via email;
- thieves stealing mobile storage devices where examination papers are being stored, thereby compromising the confidentiality and availability of the examination papers;
- viruses corrupting files on computer systems, including the examination papers, thereby compromising the integrity and/or availability of the papers.

With technology being relied upon by the role players, it is crucial that the institution addresses the threats associated with technology. Thereafter, ensure that the role players are aware of such threats, as well as ensure that they can appropriately deal with the threats. However, it is not only the threats to technology that could compromise the security of the examination papers, but the unconscious and negligent practices of role players could also contribute (Chapter 1). Consequently, those need to be addressed as well.

In order to determine and understand what exactly needs to be addressed and to understand the full spectrum of the threats and the associated risks, the institution can start by assessing the EPPP to identify the associated information security risks.

3.4 Assessing the Examination Paper Preparation Process for Risks

International best practices recommend that security efforts should be based on identified risks (Chapter 2), which could be identified through a risk assessment**.** A risk assessment is identified as the foundation of a risk-based approach for securing an information environment. It is a means of ensuring that all possible threats and vulnerabilities to the environment are addressed and accounted for. Furthermore, it is an effective process for the identification and selection of suitable security control measures (ISO/IEC 27005, 2011). It serves as basis for managing risks, from where other functions follow and decisions are made (ISO/IEC 27001, 2005).

Assessing the risks pertaining to the EPPP will assist in determining what could compromise the security of the examination papers and what the resulting consequences to the process and the institution as a whole will be, should it occur. Through the assessment the institution should be able to determine the security requirements for the EPPP. Once the security requirements are determined, the institution could then be able to decide how best to satisfy these security requirements. It will then be able to decide on appropriate actions to take based on what has been identified (Gerber, von Solms, & Overbeek, 2001). Satisfying the security requirements will ensure a secure EPPP that preserves the CIA of the examination papers. A risk assessment can assist in securing the EPPP. A risk assessment is crucial and a foundation for controlling and managing efficiently those risks that could compromise the information security of examination papers. It ensures appropriate and adequate security that protects the examination papers efficiently, by ensuring that suitable information security controls are selected and implemented based on identified risks. The information security controls are meant to meet and satisfy the determined security requirements.

Hence, assessing the EPPP for risks is the first step for securing the EPPP efficiently, as according to Stroie and Rusu (2011), a risk assessment assists in:

- providing adequate level of protection for information assets;
- establishing an acceptable level of risk;
- identifying and meeting information security requirements; as well as
- providing risk mitigation recommendations.

When assessing an environment for risks, ISO 27005 (2011) and NIST SP 800-30 (2002) suggest that a process or methodology be followed. The next section will discuss an information security risk assessment methodology.

3.5 Information Security Risk Assessment Methodology

In order to assess and mitigate risks to information security, many successful organizations recognize the significance of following a structured risk assessment process or methodology. These processes or methodologies help to ensure that information security risks are identified, discussed, understood and addressed efficiently and appropriately, in order to determine the best ways of providing protection (United States General Accounting Office, 1999). For the purpose of this research study, it will be refered to as a risk assessment methodology.

A risk assessment methodology provides a structured way of identifying the valuable assets that require protection; identifying the threats to those assets; and determining the vulnerabilities that, once exploited by the threats, could introduce risk to the organization. The identification of assets, threats and vulnerabilities are essential elements of any risk assessment methodology. Various sources, such as the McCumber Cube methodology (2005), ISO 27005 (2011), ISO 31000 (2009) and NIST SP 800-30 (2002), give assent that a risk assessment methodology should include the following activities:

- Defining of the scope and boundary - the process or system to be assessed needs to be identified, and its scope and boundary defined. This should include all the resources used for the processing, storage and tranmission of the information. The objectives and goals should be clearly defined, in order to know what the assessment aims to achieve.

- Identification of information assets – information assets that require the protection need to be clearly identified and defined, in order to understand that which is being protected. This may include making a list and placing values, so as to know which assets require the most protection.

- Identification of threats to the information assets – threats pertaining to the particular environment that is being operated in need to be identified, in order to know and understand what you are dealing with and what you are protecting against.

- Identification of potential vulnerabilities – any weaknesses to the information system that process, store and transmit the information assets need to be identified. Weaknesses to the softwares used, or weaknesses to the processes, practices and security controls that are in place, need to be identified. These weaknesses could be exploited by threats, thereby compromising the information assets. Therefore, these need to be identified in order to address them.

- Analysis of current and planned controls – this will assist in determining if the current controls are performing as planned or whether new ones will need to be identified. This will also assist in determining if new threats that have developed are covered or new controls will need to be identified to address them. This will help in ensuring that all threats and vulnerabilities are taken into consideration.

- Determination of the impact of successful exploitation of a vulnerability by a threat source – once the threats and vulnerabilities have been identified, the consequences to the organization need to be determined, should a vulnerability be exploited. This will contribute to determining the appropriate actions to be taken, especially for the largest impact.

- Determination of risk levels – this is to reveal the major risks which will require addressing first, as well as to determine whether the level of risk is acceptable or not. This could be achieved after conducting a risk analysis, which will determine the magnitude of potential consequences and the likelihood that those consequences will occur.

Performing these activities will assist in knowing and understanding the risks to the information assets of the organization, and will thus inform and guide the identification and selection of suitable security controls to mitigate these risks.

To assist in the identification of security risks to the EPPP, this research study follows the concept of the McCumber Cube methodology.

The following section will discuss the McCumber Cube Model and Methodology, followed by how it can contribute to the assessment of risks pertaining to the EPPP.

3.6 The McCumber Cube Model and Methodology

The McCumber Cube methodology is a structured process, which utilizes an information-centric approach for assessing risks. An information-centric approach is concerned with information assets, as the information goes through an ICT system. The methodology provides a means of assessing the full spectrum of threats and vulnerabilities to information assets by employing a cube model (McCumber Cube model, presented in Figure 3.2). The McCumber Cube model has the capacity to facilitaite an in-depth information assets identification, as the information moves through the ICT system, thereby being able to identify and account for all possible threats and vulnerabilities at each stage of the information movement. The McCumber Cube methodology provides a structured way of using the McCumber Cube model, and ascertains that all relevant activities for assessing risks are included in the assessment. Furthermore, the methodology is structured according to the suggestions of the NIST

SP 800-30 and ISO 27005, and expresses the essential risk elements (assets, threats and vulnerabilities) addressed by these two international standards.

Although the McCumber Cube methodology is mainly being used to assess and manage security risks in an ICT system, it was found to be applicable for assessing the information security risks in the EPPP, which is relying more and more on ICT. The reason for this is that the methodology is an information-based process, which can be applied to any information system environment. Therefore, the various elements and activities of the methodology can be applied in assessing the risks that could compromise the security of examination papers within the EPPP. The McCumber Cube model will assist by facilitating an in-depth examination paper identification as the paper moves through the process, thus helping to identify and account for all possible threats and vulnerabilities at each stage of the EPPP. Therefore, the McCumber Cube methodology can assist in providing a structured way of using the McCumber Cube model to assess the risks that could compromise the security of the examination papers, in order to determine the most efficient way of providing protection.

The following sections discuss the McCumber Cube model and methodology in detail.

3.6.1 The McCumber Cube Model

The McCumber Cube model can be employed to assess and manage risks to information security. It is an information-centric model, which is a reminder that information is the cornerstone of any information security effort (McCumber, 2005). The model is not organizationally or technically dependent; therefore it can be used in any information environment and allows security practitioners to encompass any ICT. The model is built on three key elements:

- the three information **states** (processed, stored and transmitted);
- the three basic information **attributes** (CIA); and

- the **security measures** (technology, policy and practice, and human factors)

The McCumber Cube model presents three dimensions, in order to capture the true nature of the interplay of the elements, as depicted in Figure 3.2. The foundation of the model is built as a two-dimensional matrix, with the information states (processed, stored and transmitted) positioned along the horizontal axis and the information attributes (CIA) aligned vertically. The third dimension focuses on the security measures (McCumber, 2005).

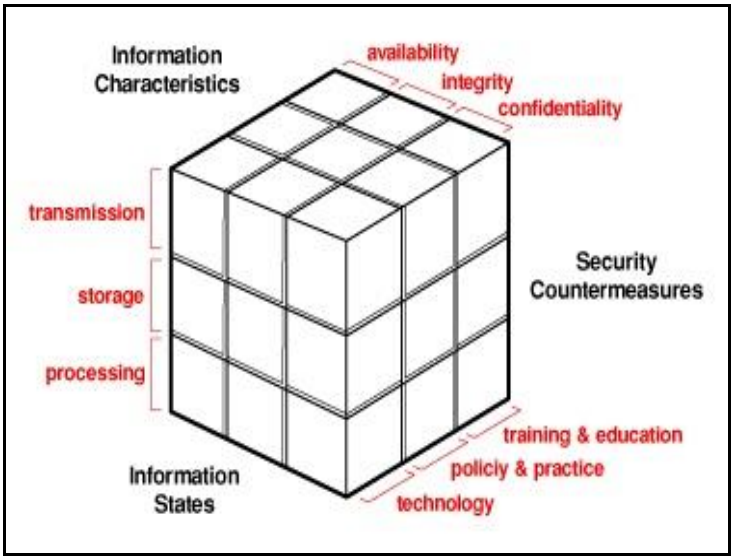


Figure 3.2 McCumber Cube Model (2005)

The two-dimensional matrix is used to identify the possible threats and vulnerabilities within the information system, while the third dimension exists to determine and identify the necessary security measures which will counteract the threats and mitigate the vulnerabilities.

To use the McCumber Cube model, one will begin by defining the various information states within the system. For each identified state, each of the information attributes is addressed by noting every possible threat and vulnerability which could compromise the security of the information attributes. Thereafter, it will be easier to work through and identify suitable security measures. For the McCumber Cube model to be employed effectively, it is recommended that it be used within the McCumber Cube methodology. The McCumber Cube methodology assists in providing a structured step-by-step process for assessing the information system environment, in order to identify the threats and vulnerabilities within that environment.

3.6.2 The McCumber Cube Methodology

“The McCumber Cube Methodology is a structured process that examines security in the context of information states” (McCumber, 2005). Central to the methodology is information, which is an asset that requires protection; hence, the fundamental nature of the information states. The McCumber Cube methodology is “designed to analyse and implement security measures that are effective in mitigating risks inherent in system and component vulnerabilities” (McCumber, 2005). However, to be able to identify suitable security measures, the information system environment and relative risks need to be assessed. The McCumber Cube methodology can thus be employed to conduct the assessment, which is carried out by defining the information states and following the information as it moves through the system.

For the assessment, the McCumber Cube methodology provides a structured way to look at the information environment in order to identify the threats and potential vulnerabilities which could compromise the security of the information assets. The results from the risk assessment can then guide the user in making sound judgements on effective security measures. To begin the assessment, the information flow will need to be defined, followed by the decomposing (separating) of the cube based on the information states and the associated information attributes (CIA). This will facilitate the in-depth identification of the various threats and potential vulnerabilities in the information system environment. Thereafter, a comprehensive security measure architecture can be developed. Table 3.1 presents the steps for the general overview of the McCumber methodology (McCumber, 2005).

Table 3.1 General Overview of McCumber Methodology

MAIN STEPS	SUB-STEPS
1. Information flow mapping.	a. Define the boundary. b. Make an inventory of all information technology resources. c. Decompose and identify all information states.
2. Cube decomposition based on information states.	a. Call out (draw out) a column from the cube – processing, storage, transmission. b. Decompose blocks by the attributes – CIA. c. Identify existing and potential vulnerabilities: i. Use vulnerability library. ii. Develop or use safeguard library. iii. Factor information value – use valuation metrics. iv. Assign appropriate safeguards in each category.
3. Develop comprehensive security architecture of safeguards (technology, procedures, human factors).	a. Describe comprehensive security architecture components. b. Cost out architecture components (including procedural and human factor safeguards).
4. Perform comprehensive risk assessment for the specific environment (if necessary).	a. Include threat and assets measurements. b. Add other implementation specific data. c. Perform cost trade-off and valuation analysis.

The McCumber Cube model and methodology can therefore be used in assessing and managing information security risks of an information system environment. The model assists in the identification of possible threats and vulnerabilities, which could compromise the CIA of information assets within the environment. The McCumber Cube model further provides for the management of the risks identified. On the other hand, the methodology provides a structural process for employing the model. The model facilitates the in-depth identification of threats and vulnerabilities, by identifying these for each state in which information exists.

As with the examination papers, it is essential that the CIA of the examination papers be preserved as the examination papers are being prepared (processed, stored and transmitted). Therefore, identifying the threats and vulnerabilities for each state of the examination papers will assist in addressing and accounting for all possible risks in the EPPP. For this reason, the McCumber Cube model and methodology have been found relevant for assessing risks within the EPPP. This will be discussed in the following section.

3.6.3 The McCumber Cube Model and Methodology for Assessing Risks in the Examination Paper Preparation Process

With the aid of the McCumber Cube model and methodology, the risks for each state of the examination papers could be addressed, by identifying suitable controls for the mitigation of these risks. This section is based on the concept of the McCumber Cube model and methodology and explains how the model and methodology can be used to identify potential threats and vulnerabilities which could compromise the security of the examination papers within the EPPP at a higher education institution.

In this study, the McCumber Cube model and methodology are found to be applicable for assessing the risks pertaining to the EPPP. Central to the model and methodology is the information that requires protection. For examination papers, being information that requires adequate protection, the model and methodology are adapted and used from the perspective of the EPPP, to identify the threats and vulnerabilities that could compromise their security. Steps 1 through to 3 of Table 3.1 are followed, as the steps are deemed sufficient for assessing the risks to the EPPP, and for identifying suitable security to counter the risks. From steps 1 and 2, information assets, threats and vulnerabilities can be identified and accounted for, at each stage of the EPPP (setting, moderation, authorization and submission). The threats and vulnerabilities include those that could be prone to the use of ICT resources used for the processing, storage and transmission of the examination papers. This will make it possible to determine the full spectrum of risks that could compromise the security of the examination papers. Thereafter, based on the risks identified, suitable security controls can be identified in step 3.

In this research study, for assessing the risks, the two-dimensional matrix of the McCumber Cube model is employed to identify the possible threats and vulnerabilities within the EPPP. The two-dimensional matrix represents:

- The three information **states** in which the examination paper exists (processed, stored and transmitted).
- The three basic information **attributes** (CIA).

The third dimension (the security dimension) will be used to identify countermeasures for the risks identified from the two-dimensional matrix.

The following is the presentation and discussion of the McCumber Cube Methodology steps, and how they are to be followed to assess the risks pertaining to the EPPP.

- **Step 1: Information Flow mapping** – This step is concerned with determining the flow of information; which is, identifying where the information is found. Information flow mapping refers to how information moves within the organization, how it is transferred from one point to another (Hibberd & Evatt, 2004). This step allows for the defining of the boundary of the EPPP. Defining the boundary is based on determining the various locations where the examination papers can be located.

This includes identifying the various ICT resources used to process, store and transmit the examination papers within the EPPP. Subsequently, each information state (processed, stored and transmitted) of the examination paper can be identified for each stage (Setting, Moderation, Authorization and Submission), as the paper flows through the EPPP. The output of this step will be a clearly defined boundary of the EPPP, an inventory of all the ICT resources used, as well as the identified information states of the examination papers. Thereafter, Step 2 follows.

- **Step 2: Cube Decomposition Based on Information States** – This step seeks to identify all possible threats and vulnerabilities that could compromise the security of the examination papers, as it moves through each stage of the EPPP. To achieve this, each information state of the examination papers and the associated basic information attributes (CIA) are dealt with separately. The cube is separated into columns based on the three information states. Each column is further divided to address each of the CIA for each of the information states of the examination papers (i.e. address the confidentiality of examination paper while being processed; the integrity while being processed, and so on). This allows for the identification of possible threats and vulnerabilities that could breach the security of the CIA for each information state of the examination papers. Thereafter, the risks can be determined as well as the information security requirements, resulting in the identification of suitable security controls to protect the examination papers.

- **Step 3: Develop Comprehensive Security Architecture Component** – This step caters for the identification of suitable information security controls based on the security risks identified in Step 2. These security controls are meant to counter and mitigate the security risks. This takes into consideration the technology, policy and procedures, as well as the human factor, in order to build a strong defence against the identified risks.

The foregoing 3 steps collectively combine into a comprehensive risk assessment for an environment, as described in Step 4 of Table 3.1, as well as defence for the environment. Therefore, the McCumber Cube model and methodology will assist in identifying and addressing all possible threats and vulnerabilities, producing a comprehensive list of possible risks. This will allow for the identification of suitable security controls that will mitigate the inherent risks resulting from the success of threats exploiting the vulnerabilities, thereby providing appropriate and adequate protection for the examination papers.

3.7 Conclusion

Examinations are a very important part of any education system, and their integrity should be safeguarded. It is for this reason that higher education institutions should ensure that their examination process is secure and that it safeguards its academic integrity, by ensuring that the confidentiality and integrity of the examinations are protected. One of the major contributors could be by ensuring that the EPPP is secure.

This chapter discussed the structure of the EPPP of a particular higher education institution, in order to assist (later in Chapter 4) in identifying the risks pertaining to such an environment. The chapter further elaborated on the importance of following a structured methodology for the assessment of any information environment, in order to comprehensively identify risks that could compromise the security of the information environment. Furthermore, the chapter identified and discussed the McCumber Cube model and methodology as suitable for the assessment of risks pertaining to the EPPP.

The following chapter discusses the practical use of the McCumber Cube Model and Methodology for assessing the EPPP, in order to determine what could compromise the examination papers within the process. This will assist in making sound decisions on how the examination papers could be suitably protected. The various methods used to collect data for the assessment will be discussed. Further discussed will be the analysis of the data, resulting in the identification of risks pertaining to the EPPP. The chapter further identifies suitable controls for the mitigation of the identified risks, in order for the examination papers to be protected.

Chapter 4

INFORMATION SECURITY RISKS ASSOCIATED WITH THE EXAMINATION PAPER PREPARATION PROCESS

4.1 Introduction

The previous chapter discussed the EPPP as one of the processes that could have a negative impact on the reputation of HEI, should the security of the process be breached. That chapter came to the conclusion that institutions should ensure that anything that could compromise the security of the process needs to be identified and dealt with appropriately; to ensure that the process is secure and that the examination papers within the process are adequately protected. Risk assessment was introduced as a means of identifying risks that could compromise the security of the examination papers. Further deliberated upon was information security risk assessment methodology for providing a structured way of assessing information security risk within an environment. The McCumber Cube methodology in conjunction with the McCumber Cube model was identified as suitable for assessing the risks pertaining to the EPPP. Further provided was a brief discussion on the steps to be followed when utilizing the McCumber Cube model and McCumber Cube methodology for assessing the security of the EPPP; in order to identify and be able to address all the possible risks pertaining to the EPPP.

This chapter follows the steps and guidance of the McCumber Cube model and McCumber Cube methodology to assess the risks pertaining to the EPPP that could compromise the security of the examination papers. From the assessment, a list of risks and a list of security controls to mitigate the risks are produced. From the identified risks, a list of information security requirements was produced, to help guide the identification and selection of security controls.

The chapter proceeds by discussing the techniques used to gather the information required to perform the assessment of the risks (Section 4.2); followed by the assessment process, where three steps of the McCumber Cube methodology will be performed (Section 4.3). Section 4.4 concludes the chapter.

The following section discusses the techniques employed to gather the required information to enable the assessment. The section further provides an explanation on what information was aimed at being elicited by the various techniques.

4.2 Data Collection Techniques

In order to carry out the assessment, certain information is required. According to NIST SP800-30 (2002), to understand the information environment that is to be assessed, there are various data collection techniques that can be employed, such as interviews, questionnaires, and document reviews. These techniques were employed in order to understand and be able to assess the security of the EPPP, in order to identify the risks pertaining to the EPPP. These techniques were introduced and referred to as research methods in Chapter 1, Section 1.7. The following sub-sections, 4.2.1 – 4.2.3 discuss the techniques and the information which the techniques aimed at eliciting.

4.2.1 Observations

In order to understand the examinations environment, the researcher spent some time at the Examinations Office, as mentioned in Chapter 1. The observation was aimed at seeing first hand how the examinations officers performed their duties when handling examination papers, as well as to observe examiners when handing in examination papers. During the observation, the researcher had conversations with the examinations officers, questioning them on their duties regarding examination papers as well as their interactions with examiners when submitting examination papers. In addition, the researcher questioned examiners regarding the examination policy, to find out if the examiners were aware of the policy and the policy contents.

4.2.2 Interviews

Two sets of interviews were conducted; the one with the Deputy Director of Examinations; and the other was with examiners, who are academic staff members responsible for setting examination papers. The interviews were aimed at getting some insight into the entire examination process, as well as the EPPP from the perspective of the Deputy Director and the examiners. The interviews were conducted to understand the structure of the EPPP and what it entails, as well as to understand the importance of security within the process.

4.2.2.1 Interviews with Deputy Director of Examinations

A semi-structured interview with the Deputy Director of Examinations was conducted in the office of the Deputy Director; an environment convenient for the Deputy Director and where the Deputy Director felt comfortable. The interview was aimed at helping the researcher understand the examination process and how the EPPP fits into the process. Furthermore, the interview aimed at understanding the purpose and aim of the EPPP, as well as what it entails. In addition, the interview aimed at understanding any security concerns of the Deputy Director, as well as find out if there are any documented policies and procedures for the process of setting examination papers. The interview questions included questions on the entire examinations process; what it entails and how the EPPP fits in; why the examinations process is structured the way it is; and whether or not any frameworks or best practices were followed when structuring the examinations process.

The interview then focussed on the process of preparing examination papers (the EPPP). This focus was to elicit more information on any available documentation on the EPPP. This was to find out if there were any documented procedures aimed at assisting the examiners in their duties in a secure manner, or if there were any other policies specific to the process. This included questions on how the examination policy is communicated to examiners, as well as on how the examinations management ensures that examiners know what is expected of them regarding the security of examination papers. The interview sheet with answers is found in Appendix B.

4.2.2.2 Interviews with Examiners

The purpose of these interviews was to get a better understanding, from the viewpoint of the examiners, of how the EPPP is structured and what it entails. The interviews further aimed at eliciting information on the ICT resources used for processing, storage and transmission of the examination papers. Unstructured interviews, in the form of informal conversation, were conducted with three randomly selected examiners as participants. This type of interview was chosen, so that the examiners would feel at ease during the interview sessions. The interviews took the form of informal conversations in a relaxed setting, during which the interviewees explained what the EPPP entailed, based on their academic experiences as examiners. There was one leading question for all the interviews: "**How are examination papers prepared? Can you please explain the process?**" Further questions referred to where the papers are set (at home or the office), and which ICT resources are used. In addition, the interviews took place to find out if the examiners were aware of the examination policy.

4.2.3 Questionnaires

Questionnaires were distributed at a particular higher education institution, to randomly selected examiners from three different departments, namely; the Nursing department, the IT department and the Business Management department. The reason for selecting participants from various departments was to get a rich sample of data from various examiners who are familiar with the examination process, from diverse academic backgrounds, and who might have different understandings and views on the securing of information and the secure use of ICT resources. A convenience sampling method was used for selecting the participants. Convenience sampling is an easy-to-get sample. It is used to select suitable people for the topic of inquiry, and the results can be generalized to the population or to any other adequately similar population (Wuensch, 2011).

The purpose of the questionnaires was to obtain information about the various ICT resources used while preparing the examination papers, as well as obtaining information on the practices of examiners. The results from the questionnaire could furthermore be used, to identify certain practices which could compromise the security of the examination papers. Fifty questionnaires were distributed, however, only 28 were returned. From these, the various ICT resources used could be identified, as well as certain practices that could compromise the security of the examination papers (and not the extent).

Participation was voluntary, and participants were informed that the questionnaires were confidential. No personal identifiable information of participants were gathered and all participants were over the age of 18. The questionnaires contained 31 closed-ended questions. Closed-ended questions mean that answer options were provided to choose from. To promote understandability, questions were divided into four categories to group related questions together. The examiners were asked questions about the ICT resources used to compile, store and transmit examination papers, as well as about the environment from which they work (office or home). For example:

- Which storage devices are used to store the examination papers? Sample option answers included: C/drive, Cloud, Flash drive

- How are examination papers transmitted to moderators or to the examinations office? Sample option answers included: Via-email or hand-delivered

- Have they ever left your office or computer screens unlocked while unattended? With option answers: Yes or No

- Do they know how to encrypt and if they do encrypt the examination papers. With option answers: Yes or No

- Do they have antivirus software installed on their home computers, and if the software is updated. With option answers: Yes or No
- Do they often scan for viruses. With option answers: Yes or No

The questionnaire is presented in Appendix C.

Various limitations of the questionnaires were identified and considered, such as the fact that the findings might not describe the actual situation precisely, as the participants may not have been openly straightforward and honest with their answers. Furthermore, in the questionnaire it is not clear whether the participants stored and backed up on the same device; as some of the participants have, for example, selected the flash drive for storing and for backup of examination papers. The analysis had to assume and cater for storing and backing up on the same device as well as on different devices. However, the recommendation was to cater to and address the adverse situation.

4.2.4 Document Review

The aim of the review was to acquire additional information on the EPPP, from official documentation of the institution. The review was to determine what is documented and to determine if that which is documented does assist examiners in performing their duties in a secure manner. Furthermore, the document review was to determine if the security of the examination papers is prominent in the documentation and to what extent. In addition, the review was to determine if the document addresses any threats that examiners should be aware of. The document reviewed was the examinations policy, which contained consolidated examination policies and procedures. The document addressed various topics and issues relating to examiners and moderators, examination venues, invigilation, graduation ceremonies, and instructions for students. However, the relevant section in the policy, which had significance to this research study, was that of examiners and moderators. Therefore, the focus of the review was on the section of the policy that referred to examiners and moderators. In addition, various elements that relate to security were reviewed.

Having discussed the information-gathering techniques and the information the techniques aimed to elicit, the following section discusses the conducting of the risk assessment based on the information gathered.

4.2.5 Literature Review

Various literature sources were consulted to gain insight and an understanding of information security risks; the assessment and management of the risks; as well as the methodologies that can be followed to determine the risks. From literature, it was established that to determine risks, threats and vulnerabilities that could compromise the security of information assets need to be identified.

To identify the threats and threat sources that may be applicable to the EPPP, standards such as the NIST SP 800-30 (2002), ISO/IEC 27005 (2011), and SANS Institute (2002) were consulted.

To identify suitable security controls, two international standards were utilized: ISO/IEC 27002 (2013) and NIST SP 800-53 Rev 3 (2009),

4.3 Information Security Risk Assessment Process

As mentioned earlier in the chapter, the assessment is based on the McCumber Cube Methodology. Steps 1 through to Step 3 of the McCumber Cube Methodology are performed for the assessment (cf. Table 3.1).

4.3.1 Step 1: Information Flow Mapping

This step is concerned with identifying the process to be assessed and determining the flow of information within the process, as well as identifying the ICT resources used to process, store and transmit the information (cf. Section 3.6.3).

The EPPP has been identified as the process to be assessed, the object being to uncover potential risks pertaining to the environment; risks that could compromise the security of the examination papers handled within the process. Thereafter, means of addressing those risks could be identified. Information used for this step is the information gathered from the interviews conducted and the document review.

Based on the information gathered from the interviews, it was determined that the EPPP consists of four stages (Setting, Moderation, Authorization and Submission) and various role players (examiners, moderators, HODs and examinations officers) are involved. During the Setting stage, examination paper would be set by an examiner or examiners collaborating on the examination paper. During the Setting stage, examiners could work on examination papers from the office and/or home. From the Setting stage, the examination paper would be transmitted to the Moderation stage, for moderation by the moderator. Once moderated the paper would be transmitted back to the examiner to update the paper based on the recommendations of the moderator, if any. From there, the paper moves to the Authorization stage to be authorised by the HOD. Thereafter, the paper is sent back to the examiner, in order for the examiner to submit the paper to the Examination officer at the Examinations office, this is the Submission stage. During the four stages, the processing, storage and transmission of the examination papers could be done electronically and/or manually. In addition, various ICT resources are used for the processing, storage and transmission of examination papers. The following ICT resources were identified:

- Processing: Computer and laptop;
- Storage: C/drive, Cloud, External hard-drive, Flash drive, Network drive, Shared drive;
- Transmission: email.

Therefore, the examination papers flow:

- Between the four stages;
- Between office and home; and

- Can be located in various ICT resources or manual resources, such as in a brief case, laptop bag, desk drawer or cabinet.

At any point in time during the EPPP, the examination papers could be in a process, stored or transmitted state. All this has to be considered in order to determine the full spectrum of the potential risks.

4.3.2 Step 2: Cube Decomposition Based on Information States

This step is concerned with identifying all possible threats and vulnerabilities that could compromise the security of the examination papers. For the examination papers to be protected, the CIA of the papers needs to be preserved. To achieve this, each column of the McCumber Cube is separated based on the three information states (processing, storage and transmission). Thereafter, each column is further divided to address each of the CIA attributes for each of the information states of the examination papers. Then finally, the threats and vulnerabilities for each combination of information states of the examination papers and the associated CIA attributes are identified (cf. Section 3.6.3). This will therefore result in the full spectrum of potential risks pertaining to the EPPP being determined, in order to identify ways of dealing with the risks so that the papers can be protected.

To identify the threats, literature sources (information security journals and standards) were consulted, and a list of possible threats to the examination papers was compiled. A threat is the combination of threat-source and threat-action; therefore, the list is presented in a tabular form based on the Threat-Source and the associated Threat-Action for each combination of information states of the examination papers and the associated CIA. Table 4.1 is a presentation of a sample list, which presents the Threat-Source along with the associated Threat-Action that could compromise the confidentiality of the examination papers during processing (Processing state). The complete list for each combination of information state and CIA is presented as Appendix D.

Table 4.1 Threat-Source/Threat-Actions for Processing State: Confidentiality

THREAT-SOURCE	THREAT-ACTIONS
Hacker	• Remote spying. • Gaining unauthorized access to information.
Intruder	• Physically gaining unauthorized access to information, by physically gaining unauthorized access to physical environment. • Opportunistically viewing confidential information.
Eavesdropper	• Eavesdropping and viewing confidential information.
Shoulder surfer	• Observing information without authorization by looking over the shoulder of another or spotting information from a distance.
Employee	• Unauthorized system access. • Negligent behaviour and practices.
Dumpster diver	• Going through dustbins to retrieve confidential information.

To identify the vulnerabilities pertaining to the EPPP, questionnaires were distributed to randomly selected examiners from three different departments of a particular HEI, namely; the Nursing department, the IT department and the Business Management department. Based on the responses, the following were identified as vulnerabilities that, once exploited, could compromise the security of the examination papers:

- Storing and backing up examination papers on the same storage device.
- Not encrypting examination papers.
- Not shredding examination papers (just throwing them in a dustbin).

- Writing down passwords on sticky notes.
- Leaving office doors unlocked and unattended.
- Leaving computer screens unlocked and unattended.
- Forgetting examination papers on shared printers.
- Not having an antivirus installed on the computer and/or laptop.
- Not updating the antivirus on a frequent basis.
- Not scanning the computer and/or laptop frequently for viruses.
- Not knowing whether or not they have open shares on the computer network.
- Not aware of the examinations policy.
- Not reading the examinations policy.

Other vulnerabilities were identified from the observation and the document review.

- From the observation, it was established that some of the examiners were not following what was in the documented policy when submitting examination papers.
- Some of the examiners did not use folders for their examination papers as documented.
- Also, some examiners will send in secretaries to submit the papers on their behalf, but they had not signed the flap of the sealed envelope so that the examinations officer can know that the envelope was not tempered with.
- In addition, examiners we asked if they were aware of the examination policy and its contents regarding preparing and submitting examination papers. Some responded

that they were aware but have not read the policy, while others were not even aware of the policy.

When questioned how they knew about the procedures to follow regarding the preparation and submission of examination papers, some said they have had been informed by their colleagues. Therefore, the vulnerabilities identified from the observation were:

- Examiners not being aware of the policy document.
- Examiners not reading and being familiar with the contents of the policy.
- Examiners not following what is documented in the policy.

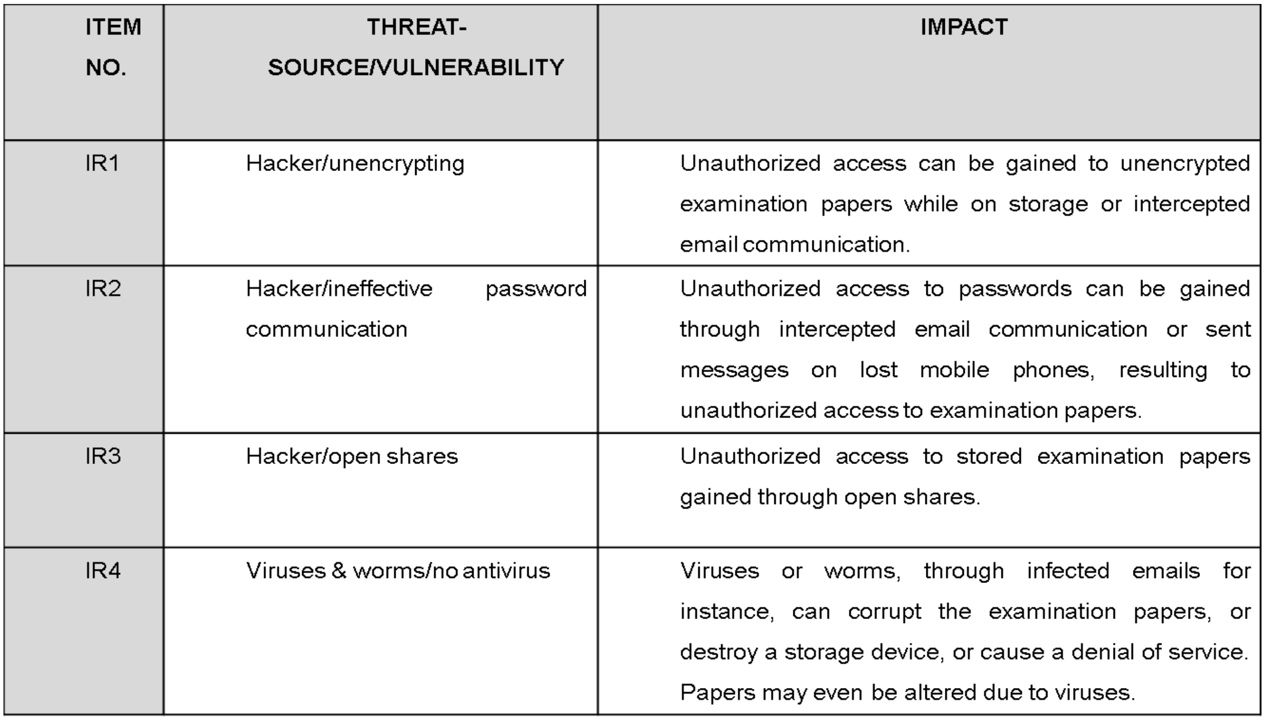
Having identified the threats and vulnerabilities, it was possible to map all possible combination of threats and vulnerabilities that could compromise the security of each combination of information state and CIA at each stage of the EPPP. This mapping assisted in identifying all possible risks pertaining to the EPPP. Table 4.2 presents a sample of the identified threats and vulnerabilities that could compromise the CIA of examination papers while being processed during the Setting stage of the EPPP. Appendix E presents the complete list of the threat/vulnerability combination for each stage of the EPPP.

Table 4.2 Threat/Vulnerability for Processing: CIA

Setting Stage			
	Confidentiality	**Integrity**	**Availability**
	Threats: • Hacker, remote spying and gaining unauthorized access to examination papers.	Threats: • Viruses and worms corrupt files/ documents/ information/ equipment and alter information.	Threats: • Viruses and worms corrupt files/ documents/ information/ equipment.

Processing State	• Intruder physically gaining unauthorized access to information, by physically gaining unauthorized access to physical environment and opportunistically viewing confidential information. • Eavesdropper eavesdropping and viewing confidential information. • Shoulder surfer observing information without authorization by looking over the shoulder of the another or spotting information from a distance. Vulnerabilities: • Leaving office doors unlocked and unattended. • Leaving computer screens unlocked and unattended. • Not keeping a clean desk policy. • Not shredding hard copies of draft examination papers.	• Intruder physically gaining unauthorized access to information, by physically gaining unauthorized access to physical environment and opportunistically make changes to confidential information. Vulnerabilities: • Not having anti-virus on computer. • Not updating anti-virus. • Not frequently scanning for viruses. • Leaving office doors unlocked and unattended. • Leaving computer screens unlocked and unattended.	Vulnerabilities • Not having anti-virus on computer. • Not updating anti-virus. • Not frequently scanning for viruses.

From the identified threats and vulnerabilities combination, potential risks were determined. Figure 4.1 presents a sample list of the potential risks pertaining to the EPPP. The complete list is presented in Appendix F.



ITEM NO.	THREAT-SOURCE/VULNERABILITY	IMPACT
IR1	Hacker/unencrypting	Unauthorized access can be gained to unencrypted examination papers while on storage or intercepted email communication.
IR2	Hacker/ineffective password communication	Unauthorized access to passwords can be gained through intercepted email communication or sent messages on lost mobile phones, resulting to unauthorized access to examination papers.
IR3	Hacker/open shares	Unauthorized access to stored examination papers gained through open shares.
IR4	Viruses & worms/no antivirus	Viruses or worms, through infected emails for instance, can corrupt the examination papers, or destroy a storage device, or cause a denial of service. Papers may even be altered due to viruses.

Figure 4.1 Risk List

From the risks identified through a risk assessment, information security requirements could be identified. These requirements are able to assist in identifying and selecting suitable security controls that will mitigate the potential risks. The level of security required is able to be determined from the requirements, and from that, a security controls architecture (a combination of technology, procedures and people) is able to be developed. The following is a list of identified information security requirements for the EPPP:

- Maintenance of confidentiality, integrity and availability of examination papers.
- Examination papers should only be accessible to authorized individuals.
- Examination papers should be free of any unauthorized modification; papers should be in the correct format with nothing altered owing to files being corrupted.

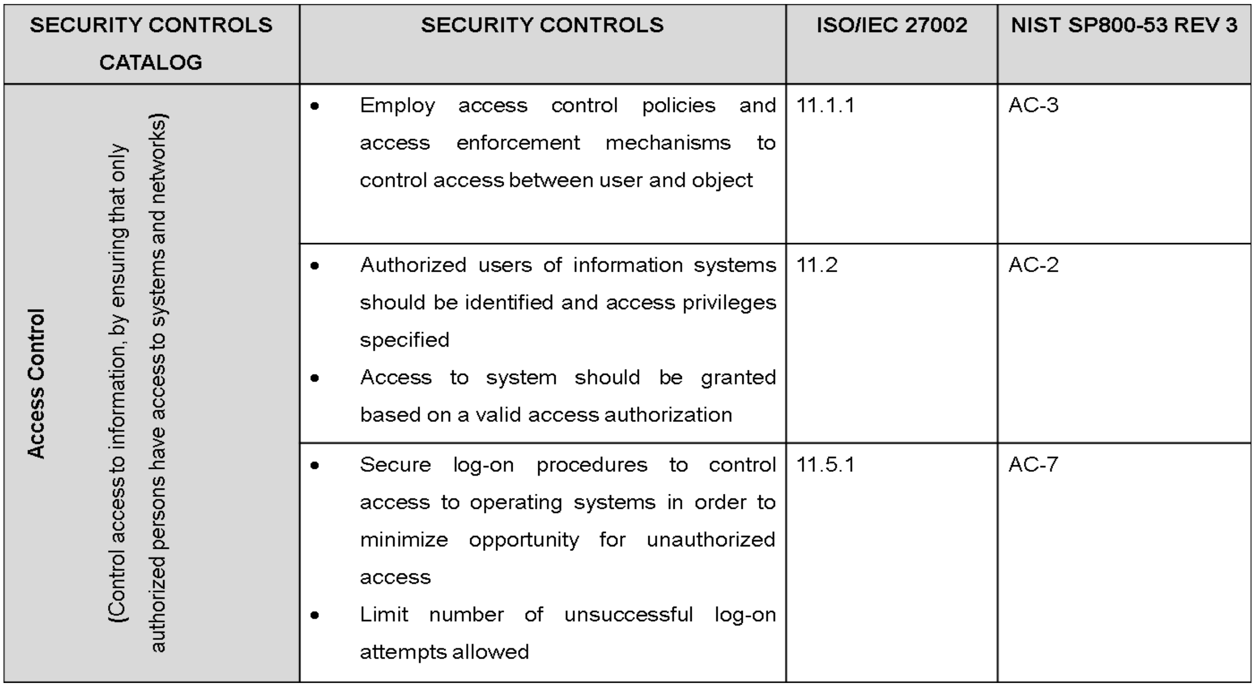
- Examination papers should always be available to authorized individuals when needed.
- Role players should be aware of threats and vulnerabilities associated with the EPPP.
- Role players should be aware of security controls in place for the mitigation of the risks.
- Security controls should be enforced.
- The examinations policy should be adequate, properly communicated to the relevant people and should be enforced.
- The role players should be aware of and have read the examinations policy before they can continue with setting examination papers.
- Role players should be made aware of the secure means of storing and disseminating examination papers (electronic or hard copies).
- Role players should be made aware of the secure use of mobile devices utilized for processing, storing and disseminating examination papers.
- Role players should be made aware of proper means of discarding/disposing draft copies of examination papers.
- Role players should be aware of behaviour or practices that could compromise the security of examination papers.

Having determined the potential risks and the information security requirements, suitable security controls can be identified.

4.3.3 Step 3: Develop Comprehensive Security Architecture of Safeguards

This step identifies suitable security controls to mitigate the risks and to satisfy the security requirements determined in Step 3. A security control architecture is developed for the security controls. A security control architecture is a combination of technology, policies, procedures, as well as people (ref. Section 3.6.3).

Literature sources, namely, books and journals, were consulted to identify the security controls as means of mitigating and managing the identified potential risks. The list of security controls were identified from two international information security standards: ISO/IEC 27002 (2013); NIST SP800-53 Rev 3 (2009). Figure 4.2 presents a sample of the security control list. Appendix G presents the complete list.



SECURITY CONTROLS CATALOG	SECURITY CONTROLS	ISO/IEC 27002	NIST SP800-53 REV 3
Access Control (Control access to information, by ensuring that only authorized persons have access to systems and networks)	• Employ access control policies and access enforcement mechanisms to control access between user and object	11.1.1	AC-3
	• Authorized users of information systems should be identified and access privileges specified • Access to system should be granted based on a valid access authorization	11.2	AC-2
	• Secure log-on procedures to control access to operating systems in order to minimize opportunity for unauthorized access • Limit number of unsuccessful log-on attempts allowed	11.5.1	AC-7

Figure 4.2 Security Controls List

4.4 Conclusion

The aim of this research study is to improve the security of the EPPP, in order to preserve the CIA of examination papers. In order to improve the security an assessment of the EPPP had to be conducted, in order to identify any potential risks that could compromise the security of the examination papers within the process. In this chapter, an assessment was conducted to identify the risks pertaining to the EPPP, in order to be able to identify security controls that will mitigate those risks. Information was gathered for the assessment, and from the information it was established that threats to examination papers exist and that some practices and behaviour of certain role players could be weaknesses that, once exploited by the threats, could compromise the security of the examination papers. Therefore, it became clear that certain things are of security concern and needed to be addressed appropriately.

The risk assessment produced a list of potential risks pertaining to the EPPP. From the risks, information security requirements were able to be identified. These information security requirements guided the identification and selection of a set of security controls to mitigate and manage the risks. These can thus assist in improving and managing the security of the EPPP, in order to preserve the CIA of examination papers.

Based on the results of the risk assessment, it became clear that a solution is required in order to provide appropriate and adequate protection for the examination papers. Therefore, the next chapter proposes a solution to help manage and improve the security of the EPPP, in order to protect the examination papers within the process. The results from this risk assessment are included in the proposed solution.

Chapter 5

INFORMATION SECURITY ASSURANCE MODEL (ISAM) FOR AN EXAMINATION PAPER PREPARATION PROCESS

5.1 Introduction

The previous chapter assessed the EPPP of a particular HEI to identify various security issues that could compromise the security of the examination papers within the process. Risks pertaining to the EPPP were identified, resulting from a risk assessment that was conducted. In addition, suitable security controls were identified for the mitigation of the identified risks. The security controls were identified from two international security standards, namely, ISO 27002 (2013) and NIST SP800-51 Rev1 (2006). With the information obtained from the previous chapters, this chapter proposes a model as a means to manage and improve the security of the EPPP, in order to protect the examination papers within the process. As discussed in Chapter 1, the primary objective of this research is to develop a model for managing and improving information security while ensuring the secure use of ICT during the EPPP at a HEI.

This chapter presents the proposed model, which could be used for creating a secure EPPP at a HEI. The model includes step-by-step general guidance for the implementation of the model, which could assist the examinations management team in implementing the model and creating a secure EPPP. The aim of the proposed model is to manage and improve the security of the EPPP, in order to protect the examination papers handled during the EPPP.

This chapter commences with a brief background towards the conception and development of the proposed model (Section 5.2). This is followed by the conception of the proposed model (Section 5.3) and the development of the proposed model (Section 5.4). Thereafter, the proposed model is introduced in Section 5.5. Finally, Section 5.6 concludes the chapter.

5.2 Proposed Model Background

The proposed model could be generic, with the intention that the model be adaptable to various processes within the examination process (since the examination process in its entirety is made up of various processes, with the EPPP being one of the processes). This will be done by determining the assessment scope, which is identifying the specific process to be assessed, thereby allowing the model to be used for that specific process. However, the proposed model includes two components, which are additional guidelines that are more specific to the EPPP.

The conception and development of the proposed model is based on: information security concepts (information security aspects; information security principles; ISMS; PDCA model), which were discussed in Chapter 2. Some of these information security concepts are more explicitly visible than others. These information security concepts are deemed necessary for assuring a secure process, as the name of the proposed model suggests: **Information Security Assurance Model (ISAM)** for an Examination Paper Preparation Process.

In the proposed model, the word “**assurance**”, featuring in the name of the model, does not imply total guarantee of security, because one can only aim for reasonable security, since security can never be totally guaranteed (Government of the HKSAR, 2008). Therefore, “**assurance**”, relating to the model, refers to the intent to give confidence that due care and due diligence have been performed to ensure that all necessary steps have been taken in order for the examination papers to be protected appropriately and adequately. The word “assurance” is defined in several dictionaries as: “something that inspires or intends to inspire confidence” (Merriam dictionary); “a positive declaration, intended to give confidence” (dictionary.com); “a statement or indication that inspires confidence” (thefreedictionary.com). Therefore, the proposed model aims to provide the examinations management team, responsible for setting the EPPP, with all the necessary steps required to give assurance that the examination papers are provided appropriate and adequate protection. The protection of examination papers could be achieved by managing and improving the security of the EPPP.

Chapters 2 and 3 contributed to the theoretical foundation of the proposed model. In Chapter 4 an assessment of the EPPP was conducted to identify certain security issues and concerns that could compromise the security of examination papers handled within the EPPP. The results from the assessment contributed towards the development of the proposed model, by contributing two supporting components. This is discussed in detail in the next section.

5.3 Proposed Model Conception

The main objective of this research is to propose a model for managing and improving the security of the EPPP in order to protect the examination papers from being compromised within the process. With the help of the information security concepts, the security of the EPPP can be managed. The information security discipline is broad and diverse, with various information security aspects to be considered, aspects which are influenced by various factors, such as, the information environment and the risks associated with that environment amongst others. This diverse nature of information security requires a robust and firm approach in order to maintain the CIA of information assets (Von Solms, 2001). This need for a robust approach (collective approach, which is able to stand adverse conditions) justifies the selection of a model as the viable artefact to address the goal of improving information security in the EPPP. A model has the characteristics of being abstract, conceptual, and technology-independent (Tomhave, 2005). For these reasons, a model can be applied to various domains of information security with minor or no alterations (Lethbridge & Laganiere, 2005)

In this study a model is "*an abstract, conceptual construct that represents processes, variables and relationships without providing specific guidance on, or practices for, implementation*" as defined by Tomhave (2005). An analysis of the definition of a model reveals that a model consists of various components, namely:

entities, relationships, and processes, and, in addition, general guidance towards achieving objectives (Tomhave, 2005; Lethbridge & Laganiere, 2005).

Models can be classified as being descriptive, prescriptive or comparative based on their focus (De Bruin, Freeze, Kaulkarni, & Rosemann, 2005).

- Descriptive models describe the components of a model.
- Prescriptive models have descriptive characteristics and go further to propose how the model can be used.
- Comparative models describe the model, prescribe how to use the model and compare an artefact based on best standards and practices of other similar entities and processes.

The proposed ISAM is classified as being a prescriptive model. It prescribes the steps and guidance on how the target users can use the model and achieve objectives, in order to manage and improve the security of the EPPP.

The following section outlines the process that was followed to develop the ISAM.

5.4 Proposed Model Development

The ISAM was developed following an iterative sequential methodology proposed by De Bruin et al. (2005). Figure 5.1 outlines the proposed generic steps to be followed when developing a model, adapted from De Bruin et al. (2005).

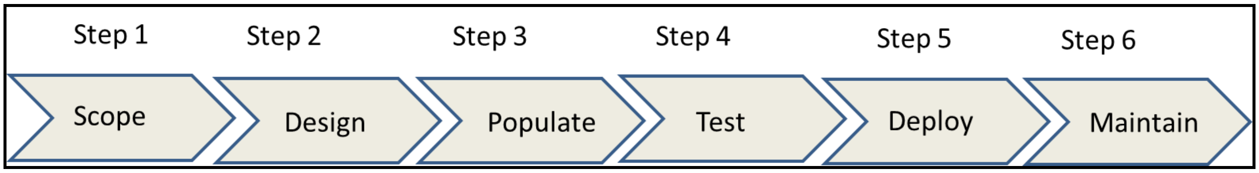


Figure 5.1: Main steps of developing a model (adapted from De Bruin et al., 2005)

A discussion on the steps and how they were applied in developing the ISAM follows. Each step starts by a paragraph describing the step according to De Bruin et al.

(2005), this is then followed by a paragraph of how the step is applied in developing the ISAM.

5.4.1 Step 1: Scoping

Scoping involves focusing the model by stating its domain of use explicitly.

The ISAM is an artefact that is aimed to be used in the domain of information security with precise focus in HEIs for the EPPP.

5.4.2 Step 2: Designing

This step refers to establishing the target user audience of the models and specifying why the users would use the model and what they will achieve from using the model. Designing ensures that the model is relevant to solving the problems of the target users.

The target users of the ISAM are examinations management team at HEIs. Their objective in using the model would be to manage and improve the security of an EPPP. By utilizing the ISAM, the examinations management team can demonstrate that due care and due diligence were performed during decision-making, as far as ensuring that examination papers are provided appropriate and adequate protection during the EPPP.

5.4.3 Step 3: Populating

Once the scope and design of the model has been clarified, the next step is to populate the model constructs (ideas for the formation of the model). Populating involves identifying the main domain concepts that are needed for the model to satisfy the needs of the target users and to solve the identified problem.

For the proposed ISAM, the theoretical base is derived from the information security discipline, as the main domain. Therefore, the information security concepts (information security aspects; information security principles; ISMS; PDCA model) were identified as the main domain concepts. The following points are a brief discussion on how the identified information security concepts were utilized for the ISAM.

- **Information Security Aspects**

  The proposed model is a guiding process which consists of various activities, which need to be performed, in order to secure the examination papers. These activities are related to various information security aspects, which are identified as relevant for the EPPP, for creating a secure information environment. The information security aspects, as discussed in detail in Chapter 2, are identified by several researchers as important considerations for any information security effort, and necessary for creating a secure information environment. These aspects will assist in ensuring that relevant information security concerns will not be overlooked, but will be considered and addressed, in order to manage and improve the security of the EPPP, and to ensure that examination papers are protected adequately and appropriately. The aspects identified as relevant for the ISAM are: **Organizational Structure, Policy; Best Practices, Risk Assessment, Human Factor, Awareness, Education and Training, and Compliance**. These aspects are not presented explicitly in the model; however, the activities related to these aspects are presented. These activities are actions that need to be carried out in order to create a secure EPPP that preserves the CIA of the examination papers.

  The Best Practices aspect is referred to as good practices or security control measures, which are security efforts that seek to provide appropriate and adequate protection for information assets. Best practices help to address security risks, and assist in formulating actions for information security requirements, identified and determined from a risk assessment process. From the risk assessment process, suitable security controls are able to be identified in order to address the risks and to satisfy the security requirements. For the EPPP a risk assessment was performed in Chapter 3. The output produced from the assessment was a list of potential security risks (**Risk List**) pertaining to the EPPP, as well as a list of security controls

(**Security Controls List**) identified as suitable for the mitigation of the risks. The two lists form part of the proposed ISAM components as supporting components

- **Information Security Principles**

The Information security principles are reflected implicitly in the proposed ISAM, as they provide the anchor that the model is based on, by providing the direction of thought that ensures that the security concerns of the EPPP are addressed. The principles include confirming that the model ensures that securing the EPPP is cost-effective, as well as that the model is based on a comprehensive and integrated approach. Information security principles are discussed in detail in Chapter 2.

- **Information Security Management System (ISMS)**

The proposed model is informed by the ISMS. As defined and described in Chapter 2, an ISMS is a management system for establishing and maintaining a secure information environment. It is 'coordinated activities to direct and control the preservation of confidentiality, integrity, and availability of information'. It assists organization to manage information security in a holistic manner, ensuring that all relevant information security aspects are taken into consideration.

The ISMS has been identified to contribute to the development of the ISAM as it will aid in the creation and maintenance of a secure EPPP; with identified coordinated activities to direct and control the preservation of the CIA of the examination papers. The proposed ISAM will further ensure that suitable security controls are selected, and that the selection is based on the results of a risk assessment, in order to provide appropriate and adequate protection for the examination papers.

- **Plan-Do-Check-Act (PDCA) Model**

The proposed ISAM will adopt the similar way the PDCA model concept is applied to the ISMS and Information Security Risk Management Process, to structure its activities (as discussed in Chapter 2). The proposed ISAM will have four phases:

1 Phase1: Plan - Establishing the plan, by identifying the objectives and determining the context.

2 Phase 2: Do - Ensuring that the plan is implemented and operates as intended, in order to achieve the objectives identified in the plan stage.

3 Phase 3: Check - Ensuring that all that has been implemented is reviewed to ensure that it is effective. This phase includes monitoring of changes.

4 Phase 4: Act - Ensuring that appropriate actions are taken based on the monitoring and reviewing.

Similar headings such as those used for the ISMS will be utilized for the phases of the proposed model. Each phase will consist of various activities. The following are the headings used for the components of each phase of the proposed ISAM: **Establish Plan (Phase 1: Plan), Implement & Operate (Phase 2: Do), Monitor & Review (Phase 3: Check), and Maintain & Improve (Phase 4: Act)**.

5.4.4 Step 4: Testing

Testing is aimed at evaluating that the model satisfies both internal and external validity. The model must conform to the foundational theoretical requirements (validity). It must also be acceptable to the intended users with respect to its components, processes and the steps for using it. Testing the model seeks to validate how well the model addresses the needs of the target users towards solving the identified problem.

The ISAM was tested using the Elite Interview method, which made use of subject domain elites in the field of information security, as well as of examinations. The elites included information security lecturers, professors and doctors from HEIs, as well as senior management staff from the Examinations Department. Chapter 6 presents the evaluation process and results of the ISAM.

5.4.5 Step 5: Deploying

The deployment step involves putting the model into use to verify its applicability and generalizability. The model should be presented to the right audience within the correct domain of model use.

The step of deploying the model could not be included in the scope of the current research study, as it requires a study that implements a longitudinal time horizon, which is not permissible within the time frame of this academic programme. The target audience (the examination management team at HEIs) will be responsible for the rollout and deployment of the ISAM.

5.4.6 Step 6: Maintaining

The model should be maintained to ensure that it is extensible and flexible to meet changing processes, standards and requirements. The model therefore needs to be maintained and kept agile in order to accommodate the changing environment. However, the scope of development of the ISAM could not include the maintenance phase owing to reasons of time horizon, as stated in the deployment phase.

The ISAM is discussed next.

5.5 ISAM

The ISAM, informed by the ISMS, is a model for creating and maintaining a secure environment for the EPPP. It consists of co-ordinated activities to direct and control the protection of examination papers within the EPPP. The ISAM aims to provide the examinations management team, responsible for setting the EPPP, with all the necessary steps and guidance required to ensure reasonable assurance that the examination papers are secure, thereby improving the security of the EPPP.

The ISAM consists of six components: four main components (Establish Plan, Implement & Operate, Monitor & Review, and Maintain and Improve) plus two supporting components (Risk List and Security Controls List). It is structured as an iterative guiding process (allowing the security of the process to be kept current, as things change and progress in the environment), consisting of various activities to be performed. The activities are divided into four phases: (Phase1: Plan, Phase 2: Do, Phase 3: Check, and Phase 4: Act), adopted from the PDCA model. The activities are actions that need to be carried out in order to create a secure EPPP that preserves the CIA of the examination papers. Figure 5.2 is a depiction of the ISAM.

A discussion of each of the six components and related four phases of the ISAM is presented next.

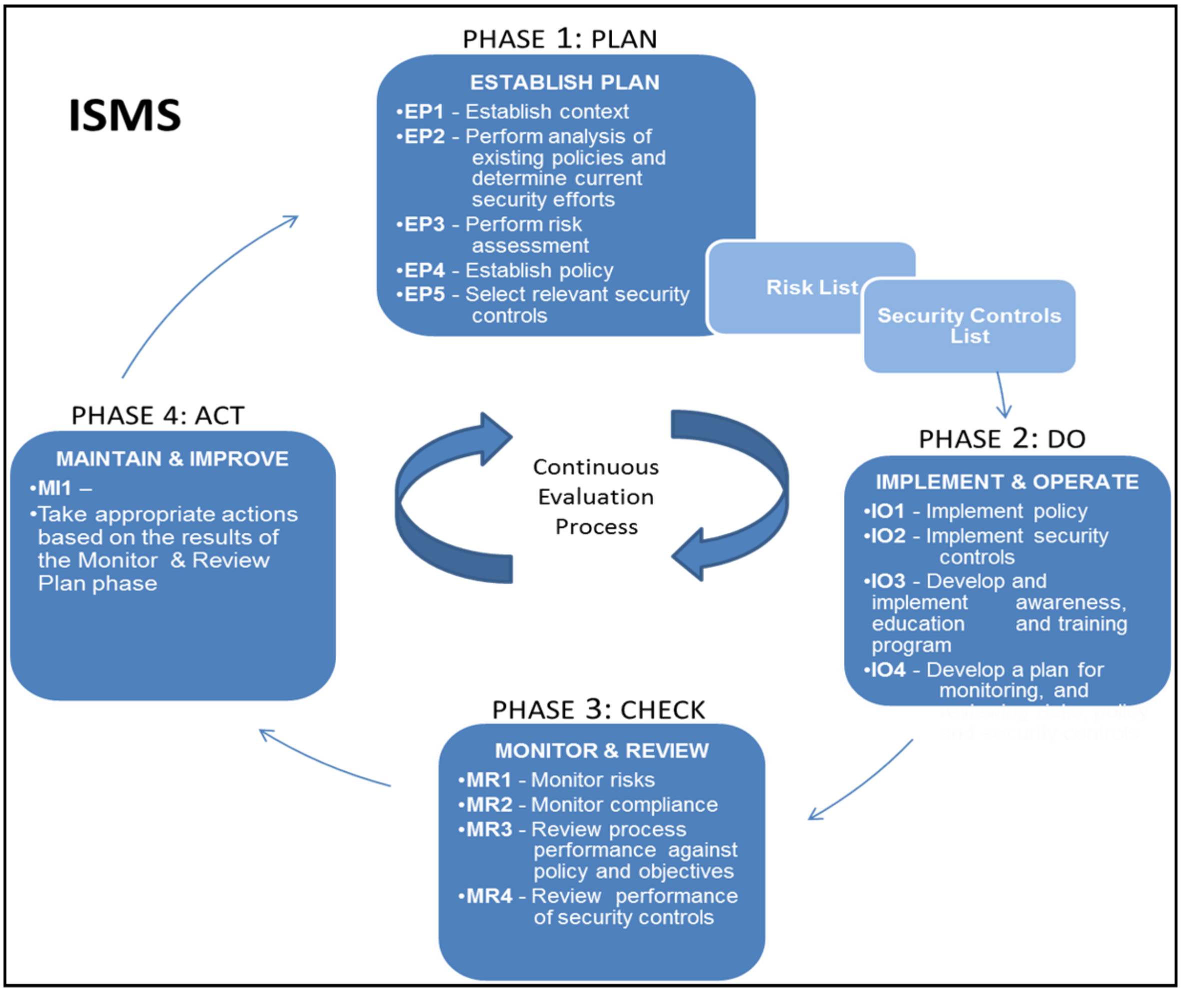
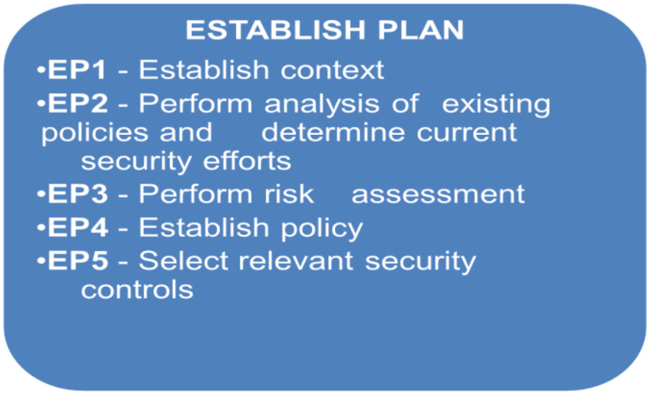

ISMS
PHASE 1: PLAN
ESTABLISH PLAN
•EP1 - Establish context
•EP2 - Perform analysis of existing policies and determine current security efforts
•EP3 - Perform risk assessment
•EP4 - Establish policy
•EP5 - Select relevant security controls
Risk List
Security Controls List
PHASE 2: DO
IMPLEMENT & OPERATE
•IO1 - Implement policy
•IO2 - Implement security controls
•IO3 - Develop and implement awareness, education and training program
•IO4 - Develop a plan for monitoring, and reviewing risks, policy and security controls
PHASE 3: CHECK
MONITOR & REVIEW
•MR1 - Monitor risks
•MR2 - Monitor compliance
•MR3 - Review process performance against policy and objectives
•MR4 - Review performance of security controls
PHASE 4: ACT
MAINTAIN & IMPROVE
•MI1 –
•Take appropriate actions based on the results of the Monitor & Review Plan phase
Continuous Evaluation Process

Figure 5.2: Information Security Assurance Model

5.5.1 Phase 1: Plan – Establish Plan

This phase is the Plan Phase of the ISAM, presenting the **Establish Plan** component. The phase is concerned with identifying the process to be assessed, and determining its scope and objectives. The phase should set the purpose and aim of the identified process, and should define its objectives, in order to give direction on how the process should exist. Thereafter, an analysis of existing policies needs to be performed, in order to determine the comprehensiveness of the policies, as well as to determine what the policies cover and to what extent. In addition, the current security efforts need to be determined, to establish what is in place for the protection of the information assets.

From there on, the identified process should be assessed, to determine any unwanted events that could deter the achievement of the objectives. Following on that should be the establishing of the policy; to help guide a consistent implementation of security controls, as well as to communicate various information security issues and concerns to relevant parties. Thereafter, suitable security controls should be identified and selected based on the results of the assessment. The security controls are meant for the appropriate and adequate protection of the valuable information assets handled within the process. The Establish Plan Component of this phase is presented in Figure 5.3.



ESTABLISH PLAN

- **EP1** - Establish context
- **EP2** - Perform analysis of existing policies and determine current security efforts
- **EP3** - Perform risk assessment
- **EP4** - Establish policy
- **EP5** - Select relevant security controls

Figure 5.3: Establish Plan Component

This phase consists of **five activities** that need to be performed.

EP1 - Establish context

EP2 - Perform analysis of existing policies and determine current security efforts

EP3 - Perform risk assessment

EP4 - Establish policy

EP5 - Select relevant security controls

5.5.2 Risk List

The **Risk List** is a supporting component. It is included as an additional guideline more specific to the EPPP, or to similar environments. The Risk List can be used, for example, by the examinations management team to identify similar risks and to support a risk assessment effort that may have been performed in Phase 1. A sample list of the identified risks is illustrated in Figure 4.1 (Chapter 4). The risks listed are potential risks that could exist in any similar process environment. Appendix F presents the complete list of the potential risks.

The Risk List is presented in a tabular form, with three columns (**Item No., Threat-source/Vulnerability, and Impact**). The **Item No.** is a unique number representing each identified risk, e.g. IR3. The **Threat-source/Vulnerability** represents a potential threat-source (Hacker) exploiting an identified vulnerability (open share) resulting in the gaining of access to valuable information by the hacker. The **Impact** represents the results of a threat-source exploiting a vulnerability, e.g. unauthorized access to stored examination papers gained through open shares.

5.5.3 Security Controls List

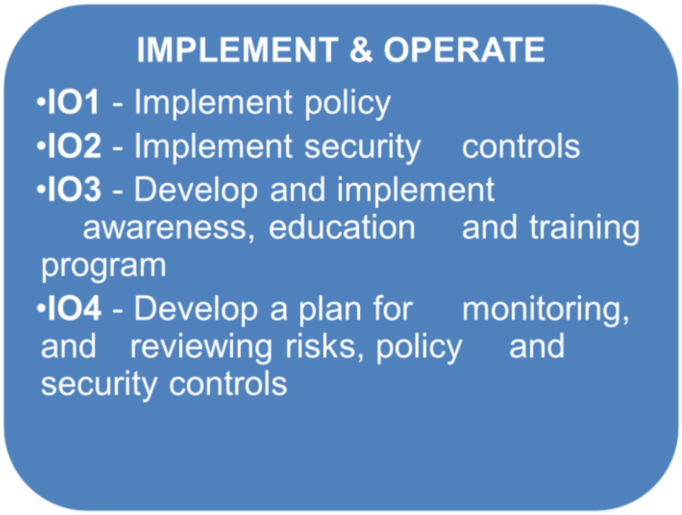
The Security Controls List is a supporting component. It is included as an additional guideline more specific to the EPPP, or to similar environments. The **Security**

Controls List can be used by, for example, the examinations management team to identify and select security controls that may be implemented to mitigate the risks identified from an assessment and presented in the Risk List, in order to protect the examinations papers. A sample of security controls included in the Security Controls List is presented in a tabular form, presented in Figure 4.2 (Chapter 4) Appendix G presents the complete list of security controls identified.

The **Security Controls List** is presented in a tabular form, with three columns (**Security Controls Catalog; Security Controls; ISO/IEC 27002; NIST SP800-53 Rev 3**). The Security Controls List is a list of security controls identified for the mitigation of the identified risks presented in the Risk List. The first column (**Security Controls Catalog**) presents the catalog and description under which the security controls fall. The second column (**Security Controls**) presents the security controls that need to be implemented. The numbering contained in the last two columns of the Security Controls List table (**ISO27002 and NIST SP-53 Rev 1 columns**), conforms to the numbering scheme of the various security controls in the two standards, respectively.

5.5.4 Phase 2: Do – Implement & Operate

This phase is the Do Phase of the ISAM, presenting the **Implement & Operate** component. During this phase, the established policy and identified security controls are implemented and operated. Furthermore, an Awareness, Education, and Training programme is developed. The programme exists to ensure that all the role players of the process know what is expected of them in regard to performing their duties in a secure manner, as well as to be made aware of the risks pertaining to the process and means of safeguarding against those risks. Figure 5.4 is a depiction of the Implement & Operate Component.



IMPLEMENT & OPERATE

- **IO1** - Implement policy
- **IO2** - Implement security controls
- **IO3** - Develop and implement awareness, education and training program
- **IO4** - Develop a plan for monitoring, and reviewing risks, policy and security controls

Figure 5.4 Implement & Operate Component

This phase consists of **three activities** that need to be performed:

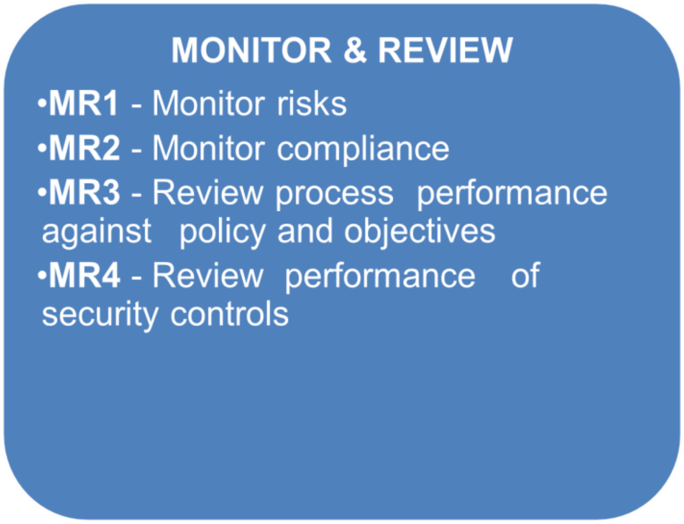
IO1 - Implement policy

IO2 - Implement security controls

IO3 - Develop awareness, education and training programme

5.5.5 Phase 3: Check – Monitor & Review

This phase is the Check Phase of the ISAM, presenting the **Monitor & Review** component (Figure 5.5). This phase ensures that the process is kept current and that risks are monitored continually, as well as to ensure that any changes are known and documented. This phase involves reviewing the policy as well as the effectiveness and operation of implemented security controls, to ensure that those operate as intended. The phase is also concerned with ensuring compliance to the policy and security controls.



MONITOR & REVIEW

- **MR1** - Monitor risks
- **MR2** - Monitor compliance
- **MR3** - Review process performance against policy and objectives
- **MR4** - Review performance of security controls

Figure 5.5 Monitor & Review Component

This phase consists of **four activities** that need to be performed:

MR1 – Monitor risks

MR2 – Monitor compliance

MR3 – Review process performance against policy and objectives

MR4 – Review performance of security controls

5.5.6 Phase 4: Act – Maintain & Improve

This phase is the Act Phase of the ISAM, presenting the **Maintain & Improve** component (Figure 5.6). This phase is concerned with ensuring that the process is always maintained, and that it stays current. The phase involves taking actions to ensure that the results of the Monitor & Review phase are implemented.

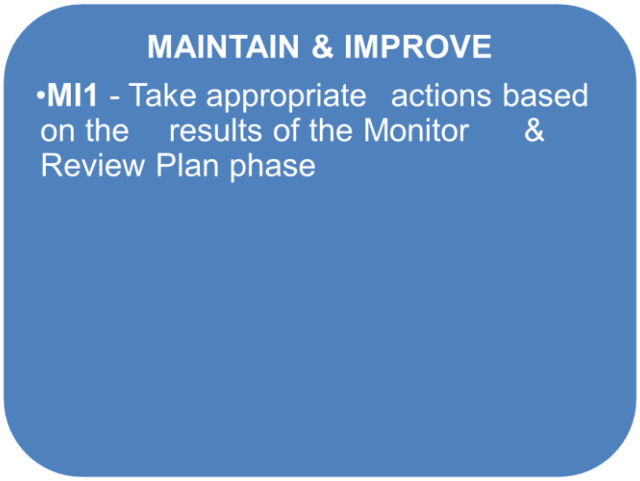

MAINTAIN & IMPROVE
•MI1 - Take appropriate actions based on the results of the Monitor & Review Plan phase

Figure 5.6 Maintain & Improve Component

The phase consists of **one activity** that needs to be performed:

MI1 – Take appropriate actions based on the results of the Monitor and Review Plan phase

5.5.7 ISAM Detailed Guide

The ISAM Detailed Guide is a separate document that provides general guidance towards the implementation of each of the phases of the ISAM.

It is a step-by-step guide, which could be followed by the examinations management team to create a secure EPPP that protects the security of the examination papers. The ISAM Detailed Guide is intended to be generic, which can be adapted with minimal effort to similar environments or other HEIs, with the aim to ensure the security of valuable information assets, such as examination papers. By following the steps, a person using the ISAM will be able to identify and select any process under consideration for assessment, and then to follow the steps of the ISAM to manage and improve the security of that specific process. Figure 5.7 only demonstrates the template of the ISAM Detailed Guide to illustrate how the guide is presented and structured. The completed ISAM Detailed Guide is presented as Appendix H.

PHASE

Description:

(Provides a short description of the phase and the purpose of the phase)

The Output of the Phase:

(Provides details of what should be accomplished at the end of the phase, the output that the phase should aim to produce)

Guiding Questions:

(Provides questions meant to assist in attaining a clear direction for the output of the phase. The questions should assist in obtaining the required information and understanding of what is being planned and how to achieve it)

Suggestions:

(Provides extra information which should be considered)

Action Plan:

(Provides the various activities of the model, which should be performed in order to achieve the output of the phase. The Action plan addresses the; What, Why, How and Who for each phase)

WHAT:	Suggests recommended action to be taken in order to assist in achieving the set objectives. (What must be done)
WHY:	Provides the purpose or aim of each of the action to be taken (the **What)**. (Why must it be done)
HOW:	Provides the contribution of the **What**, to the overall objective (improvement of security of the process or system that is being assessed. (How will it contribute)
WHO:	Identifies the various role players that should be responsible for the **What**. (Who are the role players; the responsible parties)

Figure 5.7 ISAM Detailed Guide Template

The ISAM Detailed Guide describes what should be done at each phase and what the output should be for each phase. It also includes guiding questions and suggestions. Furthermore, it provides the various actions to be taken at each phase (which are the activities to be performed). For each activity (**what**), there is an explanation on **why** the activity needs to be performed; **how** the activity can be performed; and **who** is supposed to perform the activity. For example, the ISAM

Detailed Guide will provide guidance on how a policy should be, what it should include in order for the policy to be effective.

Therefore, the ISAM, with the guidance of the ISAM Detailed Guide, will assist the examination management team to manage and improve the security of the EPPP, in order to protect the examination papers within the process. Furthermore, the examination management team will be guided in the development of the policy, as the ISAM Detailed Guide provides the information on what should be included in the policy in order for the policy to be effective.

5.6 Conclusion

This chapter proposed the Information Security Assurance Model (ISAM) for the EPPP and also outlined the process that was followed to identify the components of the proposed model. The chapter discussed in detail the various components of the model and how they have been derived from the information security discipline. The components were identified through an intensive literature study, which was described in Chapters 2 and 3, as well as through conducting an assessment of the EPPP, in order to identify potential risks pertaining to the environment. The assessment followed the guidance of an information security risk methodology.

The ISAM is meant to provide the Examinations management team with steps and activities to perform for managing and improving the security of the EPPP, in order to provide appropriate and adequate protection for the examination papers handled within the process.

The following chapter presents the evaluation process of the proposed ISAM. The evaluation of the proposed ISAM is to obtain the opinion and recommendations of the reviewers, based on their work experience and knowledge.

Chapter 6

ISAM EVALUATION PROCESS, RESULTS AND ANALYSIS

6.1 Introduction

This chapter describes the process followed to evaluate the comprehensiveness and applicability of the proposed ISAM. The purpose for the evaluation is mentioned first, explaining the details that the evaluation exercise seeks to uncover. This is followed by a discussion of the method used for the evaluation of the proposed ISAM. The findings from the evaluation are then presented. Limitations to the evaluation process are also mentioned. Thereafter, a conclusion of the chapter is presented.

6.2 Purpose of Evaluation

Evaluation is deemed a crucial component of any research process (Hevner, March, Park & Ram, 2004). In order to ensure that the proposed artifact, the ISAM, is practically useful, it must undergo stringent evaluation and justification. Evaluation aims at measuring the extent to which the artifact supports the solution to the identified problem (Peffers, Tuunanen, Rothenberger & Chatterjee, 2008). The model evaluation process aims to evaluate the relevance and rigor of the identified model constructs and content; in order to assess how well they satisfy the needs of the target audience and whether they solve the identified problem. Thus, the evaluation seeks to determine whether the components of the model are sufficient in order to aid a HEI in improving the security of the examination papers, by improving and maintaining the security of its EPPP.

This research study made use of the Elite Interview Method to evaluate the model, by obtaining the opinions and recommendations of elites, based on their work experience and knowledge. The feedback obtained from the elites was considered in order to make changes to the model, where necessary. A brief discussion on the details of the elite interview method follows. This includes presenting demographic details of the elites who participated, as well as the results obtained.

6.3 Elite Interviews

An elite interview is an evaluation method whereby a person, who is knowledgeable about the subject under investigation, is required to provide factual and practical assessment on the artifact that is being researched (Cooper & Schindler, 2003). The evaluation of ISAM made use of elites in the domains of examinations and information security. The purpose of the elite interview was to evaluate the relevance of the proposed components of the model. It also served the purpose of evaluating how the potential users of the model found the proposed model with regards to its being useful and applicable for managing and improving the security of the EPPP. The elite interview made use of a survey instrument to conduct the evaluation.

6.3.1 Survey Instrument - Questionnaires

The evaluation was conducted using questionnaires as the evaluation tool for the model, as illustrated in Appendix I and J. The review was conducted using two groups of elites (examinations elites and information security elites); therefore, the evaluation made use of two different sets of questionnaires for the two groups. The examinations elites were asked to evaluate the model based on how they find it to be applicable and useful for managing and improving the security of the EPPP. The information security elites were asked to review the understandability, completeness and relevance of the proposed components of the ISAM.

The questionnaires were structured into two categories of questions: demographic questions and utility questions. The demographic information requested to ascertain the knowledge and experience of the elites, based on their job title, job description and number of years in their current position. The utility questions were presented in the form of a three-point Likert scale rating: - disagree (1); not sure (2) and agree (3) - in response to questions regarding the utility of the ISAM.

The questionnaires were accompanied by an audio PowerPoint presentation, as well as an ISAM Detailed Guide document (Appendix H). The PowerPoint presentation was deemed convenient for the reviewers, as it takes less time to listen/view than to read. However, a document was also provided, in the event that the participants preferred reading. The PowerPoint presentation was intended to elaborate on the underlying research that formed the basis of the proposed model, as well as to explain the components of the model. The ISAM Detailed Guide is a step-by-step guiding document that is meant to support the implementation of the ISAM. The questionnaires, PowerPoint presentation and the ISAM Detailed Guide were distributed and received via email to and from the reviewers.

6.3.2 Elites

Six participants were purposively and conveniently sampled and selected from subject domain elites who represented areas of interest in the study, namely examinations at HEIs and information security. This was to gain insight from two different view points. Purposive sampling means that the researcher targeted a particular population (in this case, the examinations elites and information security elites) (Wuensch, 2011). Convenient sampling means an easy-to-get sample (in this case, the elites were accessible and in close proximity to the researcher) (Wuensch, 2011). Participation was voluntary and confidentiality was preserved.

Examinations Elites

Three senior management staff from the Examinations department at a HEI was sampled to participate as the examinations elites. These three participants represent the management and policy formulation body of the Examinations department at a particular HEI. Their role aims at ensuring the effective and efficient administration of the examination process.

Information Security Elites

Three academic lecturers in the field of information security were selected. The selection criteria for the elites were based on their contribution regarding years of experience in lecturing information security, and journal/conference publications in the domain of information security, as well as their participation in the examination process.

These information security elites also have professional affiliation, as they have titles of Doctors (Dr.) and Professors (Prof.); with the responsibilities of teaching and learning, as well as the setting and moderating of examination papers. They are also actively involved in information security-related research.

Table 6.1 presents the demographic data of the participants who were selected (the examinations elites and information security elites).

Table 6.1: Expert Reviewers' Demographic Data

Participant	**Job title**	**Job description**	**Experience (years)**	**Qualification**
Examinations Elites				
P1	Senior Examinations Officer: Postgrad	Ensure effective and efficient administration of M&Ds research assessment.	2	BTech
P2	Deputy Director – Examinations		11	MBA
P3	Senior Examinations Officer – Team Lead	Monitoring of all off-campus Examinations, involve in graduations, and setting up the examinations time table.	8	BTech
Information Security Elites				
P4	Associate Professor	Research, teaching and supervising research (Information Security).	2	PhD
P5	Senior Lecturer	Research, teaching and learning, supervising and engaging with outside	15	PhD

		entities (Information Security).		
P6	Senior Lecturer	Facilitate lectures, administration of teaching and learning aspects and community engagement (Information Security).	6	PhD

The number of years of experience of the elites ranged from 2 years to 15 years of practice in their respective domains. Such a sample of participants helped to evaluate the model in order to provide credible results, as these elites examined the components of the model and its usefulness from the perspective of how it will be applicable in their domain.

6.3.3 Presentation of Results and Findings

This section presents the results and findings of the evaluation according to the examinations elites and the information security elites, respectively. The participants were asked to rate the utility of the proposed ISAM based on Likert scale. They were also asked to provide any additional comments on the components. The results are presented in an aggregated view of the rating for each question. This is based on the count of the frequencies of how that particular question was rated on the Likert scale. First presented is the feedback from the examinations elites, followed by the feedback from the information security elites.

Examinations Elites' Feedback

The following is the feedback from the examinations elites presented in a table (Table 6.2), followed by a short discussion on the findings.

Table 6.2 Feedback from Examinations Elites

	Rating			
Question	**Disagree**	**Not sure**	**Agree**	**Comment**
From a high-level view of the ISAM; the ISAM is understandable.			3	None
The ISAM is relevant for the EPPP.			3	None
The ISAM is adaptable and can be utilized for other processes within the examination process.			3	None
The ISAM Detailed Guide provides a clear description of what needs to be accomplished at each phase of the ISAM.			2	None
The ISAM Detailed Guide provides enough information and guidance for the implementation of the ISAM.		1	1	None
The ISAM will assist in developing an adequate policy for the EPPP.			3	None
Any other comments, suggestions and/or recommendations.	"Thank you for looking at the Examinations security processes I think if we can start implementing all these processes cheating will be far low".			

The overall feedback from the Examinations elites is that the high-level view of the ISAM is understandable; relevant to the EPPP; and that it could be adapted and used for other processes within the Examinations process (all three participants agree). In the dissertation, the researcher does mention that the proposed model could be generic, with the intention that the model could be adaptable to various Examinations processes. However, the model includes two components, which are additional guides (Risk List and Security Controls List) that are more specific to the EPPP.

Pertaining to the ISAM Detailed Guide, two participants agree that it provides a clear description of what needs to be accomplished, as well as that it provides enough information and guidance for the implementation of the ISAM. The other participant did not give a rating.

Furthermore, all three participants agree that the ISAM will assist in developing an adequate policy for the EPPP.

Therefore, based on the feedback, it can be argued that the ISAM, along with the ISAM Detailed Guide, is understandable and can assist the Examinations management team in defining and documenting a secure EPPP, if the guide is followed in detail.

Information Security Elites' Feedback

This section is the presentation of the feedback from the information security elites in a tabular form (Table 6.3), followed by a discussion of the findings.

Table 6.3 Feedback from the Information Security Elites

	Rating			
Question	**Disagree**	**Not sure**	**Agree**	**Comment**
From a high-level view of the ISAM; the ISAM is understandable.	1		2	• ISAM is understandable. • However, I fail to understand where and by whom the ISAM will be used .
From high-level view the ISAM is relevant for the EPPP.			3	• Relevant although actual implementation may be challenging and time consuming.

				• I would like to know whether the applicability based on the context is explained elsewhere. • It is generic enough, what about it is specific to the EPPP.
The ISAM comprehensively identifies crucial components that contribute to a secure EPPP.	1	1	1	• The ISAM has identified crucial components that contribute to a secure EPPP during processing, storage and transmission. • There is nothing that I can see in the ISAM that specifically or comprehensively addresses a secure EPPP, its generic. • I feel it is not out of the scope of this work, external examiners should be listed as role players also.
The ISAM can assist in defining and documenting a secure EPPP.			3	• At a high-level. • It could possibly assist someone in documenting a secure EPPP.
The ISAM can assist in the development of a	1		2	• If EP4 is followed in

policy specific for the EPPP, which clearly addresses the security of the examination papers.				detail. • Yes this model does cater for it. • Phase 1 of ISAM EP4 indicates that a policy must be established. Therefore, the ISAM highlights that a policy is needed, but I do not think that this will assist in the development of a policy.
The ISAM can assist in creating and raising awareness of any security related issues pertaining to the EPPP, for all stakeholders.	1		2	• I would love to read the results of test done on the applicability. • The ISAM simply suggests that a Awareness program is needed, however, who will develop the program, who will run it, who needs to attend.
Any other comments, suggestions and/or recommendations.	• Successful implementation of ISAM will require the buy-in from all the relevant stakeholders. In addition some special skills may be required. • How will the process be monitored and by whom? How will the ISAM assist in assuring the Examinations Department that I have followed a secure process? Who will monitor me at home? • I feel the clarification of this model could be assisted by a thorough example of how the process would work – detailing			

	role players and responsibilities.

All three of the information security elites agree that the ISAM is relevant for the EPPP and can assist in defining and documenting a secure EPPP. In addition, all three elites were positive that the ISAM will contribute in improving and maintaining security of the EPPP, in order to provide adequate protection for the examination papers. However, a number of concerns regarding the ISAM were also raised. The concerns follow with a brief discussion of how the concerns are addressed:

- One participant felt that as much as the ISAM Phases are understandable, it is not clear where and by whom the ISAM will be used: ***"Initially I thought it was for the examination department to attempt to ensure the CIA of exam papers. But then further in the presentation, it was inferred that the ISAM was for use by examiners and moderators. And only the internal moderators – the external examiners are not taken into account at all"***

  The target audience for the ISAM is the Examinations management team. This is mentioned in the PowerPoint presentation ('the proposed model aims to provide the Examinations management team responsible for setting the EPPP with all the necessary steps required to give assurance'). This is further mentioned in section 5.4.2 of the dissertation.

  "Also, the presentation mentioned that 'role players' will be responsible for the Phases of ISAM. Who is responsible for which Phase?"

  Examiners and moderators are mentioned as 'role players – those involved in the EPPP – who, while preparing examination papers, need to take note of their practices'. Role players are also mentioned as the group that will need to be made aware of risks pertaining to the EPPP, as well as the controls aimed at mitigating those risks. Therefore, the Examinations management team is the responsible party for implementing each Phase of the ISAM, supported by the guidance of the ISAM Detailed Guide, the step-by-step guide.

"Who establishes the Risk List and decides which Security Controls are applicable?"

The Risk list and the Security Controls List are the output results of a risk assessment conducted on the EPPP. The Examinations management team is responsible for ensuring that a risk assessment is conducted, and professionals can be sought to assist. This is stated in the ISAM Detailed Guide (ref: ISAM Detailed Guide: EP3 – Perform Risk Assessment).

However, the other two participants were in agreement that the ISAM was easy to understand.

- Although all participants agree that the ISAM is relevant for the EPPP, one of the participants felt that it was generic. ***"it is generic enough that it could be used for many information security assurance applications. What about ISAM is specific to EPPP"*** and ***"There is nothing that I can see in the ISAM that specifically or comprehensively addresses a secure EPPP. It identifies components that are generic for almost any form of information assurance."***

  As generic as the components are, they can be applied to the EPPP as means to ensure that the security of examination papers is preserved. Through the components, any security issues can be addressed comprehensively. In addition, the ISAM includes two other components as additional guidelines, which are more specific to the EPPP (Risk List and Security Controls List). The Lists are the output of a risk assessment conducted on the EPPP; therefore they address risks pertaining to the EPPP and how to counter those risks.

  One other participant raised concerns that the ISAM does not include external examiners and moderators. The reason for this is that the external examiners and moderators are outside the scope of the study, as the papers go via the Examinations office, and the study concentrated on the process just up to reaching the Examinations office.

- Two of the participants agreed that the ISAM can assist in developing a policy that addresses security, the other participant felt it does not address the development of a policy: ***"In Phase 1 of the ISAM, it is indicated by EP4 that a policy must be established. Therefore, the ISAM highlights that a policy is needed, but I do not think that this will assist in the development of the policy."***

  A policy is written to support the aims and objectives of an identified process, and specifies and dictates acceptable and unacceptable behavior for all role players involved in the process. It provides a set of rules for the protection of information assets within the process, and directs how issues should be addressed. The ISAM, with the support of the ISAM Detailed Guide, will assist in defining the objectives and in identifying security concerns that need to be addressed. Furthermore, the ISAM Detailed Guide provides guidance on what is required in order for the policy to be effective (ref: ISAM Detailed Guide: EP4 – Establish Policy).

- Two of the participants agreed that the ISAM can assist in creating and raising awareness, while one of the participants does not agree*: **"Part of ISAM (Phase 2) includes an Awareness, Education and Training Program. The program may increase awareness of security related issues. However, ISAM simply suggests that this is needed. Who will develop this program? Who will run the program? And who need to attend this? How often? Who decides this?"***

  All the questions raised regarding the Awareness, Education and Training program are addressed in the ISAM Detailed Guide (ref: ISAM Detailed Guide: IO3 - Develop and Implement Awareness, Education and Training Program).

- One participant was concerned that the presentation was inconsistent: ***"The presentation is inconsistent for Phase 2 of the ISAM. The slides indicate that there is an IO4 – but this is not discussed."***

  This is an oversight on the part of the researcher. The audio part did not discuss the IO4; however, the discussion is provided on the slide notes.

- One participant stated: ***"The ISAM Phase 3 says that the process must be monitored – how will this be done? Who will do this? If I hand in an exam paper – how will the ISAM assist in assuring the exams department that I followed a secure process? Who will monitor me at home? Having policies and processes in place does not guarantee information security assurance."***

  The ISAM Detailed Guide provides answers regarding monitoring; how it could be done and the responsible parties (ref: ISAM Detailed Guide: Phase: Monitor & Review). In addition, the ISAM will assist by ensuring that a well-defined process is in place; by assisting the Examinations management team in ensuring that documentation is in place and is properly distributed to role players, in order to be aware and to understand what they need to take into consideration when preparing examination papers, in order to preserve the security of the papers. This documentation will ensure that the role players are equipped with the means to deal with any security concerns, and that they are aware and conscious of their behavior and practices.

Overall, based on the feedback from the information security elites, it can be argued that the ISAM, along with the support of the ISAM Detailed Guide, can assist in managing and improving the security of the EPPP, in order to protect the examination papers within the EPPP. Furthermore, it can be argued that the ISAM components address the 'WHAT' that should be in place in order to ensure a secure process, like any other information security assurance framework. Then the ISAM Detailed Guide addresses the 'HOW', which helps to support and implement the 'WHAT'.

In addition to the elite interview, an academic publication was submitted and presented at an Information Security-specific conference (Appendix A). The review of the publication from such a conference with reviewers who are experts in the field of information security yielded valuable results with respect to the validation of the model.

6.4 Limitations

Various limitations, which could have influenced the results of the evaluation, were identified. These are as follows:

- The oversight of the researcher in including more detailed information and background as part of the elite interview request.
- Potential misinterpretation of details by the expert owing to the potential incomprehensiveness of the PowerPoint presentation.
- Oversight on the part of the elites, owing to overlooking certain core documents, such as the ISAM Detailed Guide.

6.5 Conclusion

This chapter discussed the evaluation of the proposed ISAM for the EPPP. It further discussed the approach that was taken to perform the evaluation, together with the feedback provided by the participants.

The concerns of the participants were also discussed and addressed. The proposed model was accordingly refined from its initial design to incorporate the feedback of the participants.

As the evaluation shows, the ISAM components were approved by the elites. Further confirmed was that the proposed model would indeed contribute to improving and maintaining the security of the EPPP; if followed in detail.

Chapter 7

CONCLUSION

7.1 Introduction

This research study focused on an effort to improve the security of examination papers at a HEI, during the process of preparing the examination papers. Through an information security risk assessment process at a particular HEI, it was determined that various risks exist, including the behaviour and practices of certain role while preparing examination papers, which could compromise the security of the papers. What was further determined, was that not having adequately documented policies and procedures in order to help address security concerns and help guide the manner in which examination papers should be handled by all role players could be a risk to the security of the papers. Therefore, the aim of this research study was to propose a way of ensuring that security concerns could be identified and addressed systematically, to ensure that the examination papers and the process are provided with the needed protection. As a result, a model for managing and improving the security of the EPPP was proposed. This model was presented in Chapter 5 and evaluated in Chapter 6.

This chapter provides the accomplishment of the research objectives, by revisiting the research objectives identified in chapter 1, to evaluate whether the objectives were met. Thereafter, this chapter acknowledges the research limitations, as well as suggesting possible future research. The chapter further discusses the significance of the research study. The Chapter concludes with a final word.

7.2 Accomplishment of Research Objectives

This section discusses the aim of this research study, as well as how the research objectives were addressed and met in order to accomplish the research aim. The aim of the research and the objectives were introduced in Chapter 1.

Chapter 1 started by introducing the background of the research study. Chapter 1 also established that examinations play a fundamental role in higher education, as they are means by which HEIs can obtain evidence of the competence of students. Therefore, it is essential that the integrity of examinations is preserved, by ensuring that examination papers are not illegally obtained by students, amongst other things. From this chapter it became clear that certain behavior of role players during the process of preparing examination papers could compromise the security of the papers. As a result, allowing the papers to be accessible to unauthorized individuals; could result in qualifications being awarded to undeserving students. This led to the discussion of the problem background, drawing attention to ***the current uncontrolled and unmanaged manner in which examination papers are being prepared (compiled, stored and transmitted) by role players, which could compromise the security and integrity of the EPPP, the examination process, and the reputation of the university as a whole***. Based on the identified research problem, research objectives were formulated to address said research problem. Further discussed in Chapter 1 was the research methodology employed to accomplish the objectives.

As stated in Chapter 1 (Section 1.6), the primary objective of this research study was to propose a model for managing and improving security and for the secure use of ICT during the Examination Paper Preparation Process at a higher education institution. To address the primary objective, the following sub-objectives had to be addressed:

- To determine the current security state of the Examination Paper Preparation Process at a particular higher education institution, including identifying policies and procedures relevant to the process.

- To identify relevant information security aspects and applicable information security principles from existing information security best practice frameworks and standards that need to be considered, to contribute towards a secure Examination Paper Preparation Process at a higher education institution.

- To integrate the identified information security aspects and information security principles, in order to contribute towards the development of a model for managing and improving the security of the Examination Paper Preparation Process at a higher education institution.

The first sub-objective: ***To determine the current security state of the Examination Paper Preparation Process at a particular higher education institution, including identifying policies and procedures relevant to the process;*** was addressed in Chapter 3 and Chapter 4, with the guidance of Chapter 2 (which helped the research to understand what information security entails; in order to know what to look for when exploring the EPPP, in terms of information security). To accomplish this sub-objective, the EPPP had to be explored, in order to understand how it is structured and what it entails. Chapter 3 provided that information, through a literature review and interviews with the Head of Examinations and academic staff members (who are also examiners) at a particular HEI. From the information obtained, the EPPP was modelled in order to understand the flow of the process and the information within the process. What was further identified was the Examination policy and procedure document relevant to the EPPP. Furthermore, it was established that various ICT resources were utilised when preparing examination papers; which provided a convenient way of preparing examination papers, as examiners were able to work both at the office and remotely. In addition, examiners were able to collaborate in a quick and efficient way when setting papers.

Thereafter, in Chapter 4 an information security risk assessment was performed, in order to determine the security state of the EPPP. From literature, the McCumber Cube Methodology was identified as suitable for performing the risk assessment. Interviews, questionnaires and a document review were used to gather the required information for the risk assessment. From the information obtained, it was identified that the practices of certain role players while preparing examination papers could compromise the security of the paper. Further identified was that the extent to which security addressed in the documented policy was not sufficient. The output from Chapter 4 was a list of risks pertaining to the EPPP, as well as information security controls that could be implemented for the mitigation of the risks (the security controls were identified from two international information security standards). Therefore, from this chapter it became clear that the security of the EPPP needed to be improved and to be managed better.

Chapter 2 addressed the second sub-objective: ***To identify relevant information security aspects and applicable information security principles from existing information security best practice frameworks and standards that need to be considered, to contribute towards a secure Examination Paper Preparation Process at a higher education institution.*** Chapter 2 recognized how most organizations have come to rely on ICT for the processing, storage and transmission of valuable information, and how information security has come to play a vital role in protecting information assets. It was established that to protect information assets appropriately and effectively, various information security aspects need to be considered and incorporated into an information security framework. The following are the information security aspects identified as relevant to contribute towards a secure EPPP: organizational structure, policy, best practices, risk assessment, awareness, education and training, human factors, as well as compliance. To be able to address and incorporate these aspects into an information security framework, it was determined that various information security principles had to be considered. Information security principles provide an approach for planning and setting an information security plan, and assist in maintaining and connecting information security within business functions. Various information security principles were identified, which were considered applicable to contribute to a secure EPPP.

The third sub-objective: ***To integrate the identified information security aspects and information security principles, in order to contribute towards the development of a model for managing and improving the security of the Examination Paper Preparation Process at a higher education institution***; was also addressed in Chapter 2. It was determined that to achieve appropriate levels of security depended on a multi-faceted system, which covers various relevant information aspects and that is informed by various information security principles. The ISMS was identified as that system, within which the protection of information assets is directed and controlled through coordinated activities. Through the ISMS, the relevant information security aspects and the applicable information security principles are integrated in order to assist in establishing and maintaining a secure information environment. Thus, the ISMS was identified to contribute to the development of a model for managing and improving the security of the EPPP.

Once the sub-objectives had been addressed, the researcher was able to address the primary objective: ***Proposing a model for managing and improving security and for the secure use of ICT during the Examination Paper Preparation Process at a higher education institution***. In view of the ISMS; which integrates the information security aspects and the information security principles, the Information Security Assurance Model (ISAM) for an EPPP was developed and addressed in Chapter 5. It was argued that the ISAM will contribute to managing and improving the security of the EPPP, in order to protect the examination papers within the process. The ISAM is a guiding process informed by applicable information security principles and consisting of the relevant information security aspects (the aspects presented as activities of the model). The ISAM adopts the PDCA model to structure the activities of the ISAM.

Consequently, the model was evaluated in Chapter 6. The chapter discussed the evaluation approach and the feedback from the evaluation. On the basis of the evaluation, the proposed model was considered sound for maintaining and improving security of the EPPP.

7.3 Significance of Research Study

Any department that works with any kind of valuable information assets needs to be aware of and to understand the value of information security in providing the necessary protection for those information assets. Information security is valuable, as it helps people to understand that the protection of information is not only about technical controls, but includes management and operational controls. Following the advice of international information security frameworks and standards is beneficial and is a step towards creating a secure information environment that provides the necessary protection for the valuable information assets within the environment.

Therefore, the significance of this research study lies in contributing towards a secure EPPP that protects the examination papers within the process; by introducing the Examinations management to the benefits of information security in providing the necessary protection for the examination papers (as information security has mostly been considered to address technical security issues).

7.4 Research Limitations and Future Research

This research study focused on internal role players (internal examiners, internal moderators and Examinations staff). External examiners and moderators were not included, as the study explored the EPPP only to the point where examination papers were submitted to the Examinations office and not beyond. At the particular HEI used as the case study, the examination papers are sent to external moderators via the Examinations office, and that part was not explored as it fell beyond the scope of the study. Furthermore, the study focused on three departments for distributing questionnaires; as those were the departments available at that point in time.

This study has provided a guiding process for Examinations management to follow in order to manage and improve upon the security of the EPPP; by incorporating information security concepts, principles and aspects for addressing risks pertaining to the process. These risks include those pertaining to the use of ICT resources for the processing, storage and transmission of examination papers. The study identified components that constitute the proposed ISAM for an EPPP. Possible directions for future research include a detailed practical implementation of the proposed ISAM. In addition, it could be used to determine how precisely a policy can be developed and communicated with the assistance of the ISAM.

7.5 Epilogue

ICT resources and the Internet have become a part of the way in which many people perform their duties and communicate. Institutions, such as HEIs, have also embraced ICT and the Internet for their business processes and collaborations on business projects with other institutions around the world. As such, examiners have come to rely on ICT when preparing their examination papers. However, there are various threats to the information which comes with the use of ICT, which could place the examination papers at risk. Therefore, it is imperative that examiners are made aware of these risks. This includes them being made aware of their practices and behavior while preparing examination papers, which could compromise the security of said examination papers, as well as ensuring that adequate policies are developed and distributed.

In the interest of preserving the integrity of the examination papers at HEIs, the process in which examination papers are prepared needs to be well managed, by ensuring that all security concerns are addressed in an efficient and effective manner. This research study developed and evaluated an ISAM for an EPPP that will contribute to managing and improving the security of EPPP, in order to provide adequate protection for examination papers. Improving the security of the EPPP could further help to guard the integrity of the qualifications awarded by the institutions, further guarding the reputation of the institutions, which will in turn help to guard the reputation of the institutions.

REFERENCES

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security*, 276-289.

Alwi, N. H., & Fan, I.-S. (2010, June). E-learning and information security management. *International Journal of Digital Society (IJDS), 1*(2), 148-156.

Anand, S. (2008). Information Security Implications of Sarbanes-Oxley. *Information Security Journal, 17(2)*, 75-79.

Anderson, G. J. (1998). *Fundamentals of Educational Research.* London: Falmer Press.

Ashenden, D. (2008). Information security management: A human challenge? *Information Security Technical Report, 13*(2008), 195-201.

Barnard, L., & von Solms, R. (2000). A formalized approach to the effective selection and evaluation of information security controls. *Computers & Security, 19*(2), 185-194.

Chadwick, D. W., Tassabehjie, R., & Young, A. (2000). Experiences of using a public key infrastructure for the preparation of examination papers. *Computers & Education, 35(2000)*, 1-20.

CHE. (2007, August). *Review of higher education in South Africa.* Retrieved June 23, 2013, from CHE: Council on Higher Education in South Africa: http://www.che.ac.za

Collis, J., & Hussey, R. (2009). *Business research: A practical guide for undergraduate and prosgraduate students.* London: Palgrave Macmillan.

Colwill, C. (2010). Human factors in information security: The insider threat - Who can you trust these days? *Information Security Technical Report*, pp. 1-11.

Cooper, D. R., & Schindler, P. S. (2003). *Business research methods.* New York: McGrew-Hill Companies.

Council of Higher Education. (2009). *Higher education monitor: The state of higher education in South Africa.* Pretoria: Council of Higher Education.

De Bruin, T., Freeze, R., Kaulkarni, U., & Rosemann, M. (2005). Understanding the Main Phases of Developing a Maturity Assessment Model. *Australasian Chapter of the Association for Information Systems* (pp. 8-19). Australia, New South Wales, Sydney: Australasian Conference on Information Systems (ACIS).

Department of Education. (1997, July 24). A programme for the transformation of higher education. *Education White Paper 3*. Pretoria, Gauteng, South Africa: Department of Education.

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

Doherty, N. F., Anastasakis, L., & Fulford, H. (2009, December). The information security policy unpacked: A critical study of the content of university policies. *International Journal of Information Management, 29*(2009), 449-457.

Eloff, J. H., & Eloff, M. M. (2005). Information Security Architecture. *Computer Fraud & Security, 11*, 10-16.

Eloff, J., & Eloff, M. (2003). Information Security Management - A New Paradigm. *SAICSIT*, (pp. 130-136).

Eloff, M. M., & Von Solms, S. H. (2000). Information security management: A hierarchical framework for various approaches. *Computers & Security, 19*, 243-256.

Ethics Resource Center (2011). *Building a corporate reputation of integrity.* Retrieved May 23, 2013, from ERC: http://erc.webaircom/files/u5/integrity.pdf

FIPS PUB 200. (2006). *Minimum security requirements for federal information and information systems.* Washington, USA: U.S. Department of Commerce.

Forte, D. (2000, March 1). Auditing and security policy: The cornerstone of company information protection. *Network Security, 2000*(3), 12-13.

Furnell, S. M., Gennatou, M., & Dowland, P. S. (2002). A prototype tool for information security awareness and training. *Logistics Information Management, 15*(5), 352-357.

Furnell, S., & Thomson, K. L. (2009). From culture to disobedience: Recognising the varying user acceptance of IT security. *Computer Fraud & Security, 2009*(2), 5-10.

Galliers, R. D., & Leidner, D. E. (2003). *Strategic information management: Challengies and strategies in managing information systems* (Third edition ed.). Oxford.

Gerber, M., & Von Solms, R. (2005). Management of risk in the information age. *Computers & Security, 2005*, 16-30.

Gerber, M., von Solms, R., & Overbeek, P. (2001). Formalizing information security requirements. *Information Management & Computer Security, 9*(1), 32-37.

Government of the HKSAR. (2008, February). *An overview of information security standards.* Retrieved October 14, 2015, from InfoSec: http://www.infosec.gov.hk

Graziano, A. M., & Raulin, M. L. (2000). *Research methods: A process of inquiry* (4 ed.). Boston: Allyn & Bacon.

Henning, E. (2004). *Finding your way in qualitative research.* Pretoria, SA: Van Schaik Publishers.

Hennink, M., Hutter, I., & Bailey, A. (2011). *Qualitative research methods.* London: SAGE Publications Ltd.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quartely*, 75-105.

Hibberd, B. J., & Evatt, A. (2004). Mapping information flows: A practical guide. *The Information Management Journal*, 58-64.

Hofstee, E. (2006). *Constructing a good dissertation.* Sandton, SA: EPE.

Hone, K., & Eloff, J. H. (2002, October 1). Information security policy - What do international information security standards say? *Computers & Security, 21*(5), 402-409.

Hone, K., & Eloff, J. H. (2002, June 1). What makes an effective information security? *Network Security, 2002*(6), 14-16.

Hong, K.-S., Chi, Y.-P., Chao, L. R., & Tang, J.-H. (2003). An integrated system theory of information security management. *Information Management & Computer Security, 11*(5), 243-248.

Howard, B., Paridaens, O., & Gamm, B. (2001). *Information Security: threats and protection mechanisms.* Retrieved 9 6, 2011, from http://lt.fe.uni-lj.si/gradiva/kos/clanki_pdf/28-information%20security%20-%20threats%20and%20protection%20mechanisms.pdf

IEASA (2011). *The guide to South African higher education: Africa & the knowledge economy.* Pretoria: IEASA

ISACA. (2012). *COBIT 4.1: Framework for IT Governance and Control*. Retrieved June 6, 2012, from ISACA: http://www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx

ISF. (2010). *Principles for Information Security Practitioners.* Retrieved October 23, 2013, from ISACA: www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/Pages/Security-Principles.aspx

ISF. (2010). *Principles for Information Security Practitioners: An Overview.* Retrieved October 23, 2013, from Information Security Forum: www.securityform.org

ISO/IEC 27000. (2009). *Information technology - Security techniques - Information security management system - Overview and vocabulary.* Geneva: International Organization for Standardization.

ISO/IEC 27001. (2005). *Information technology - Security techniques - Information security management system - Requirements.* Geveva: International Organization of standardization.

ISO/IEC 27002. (2013). *Information technology - Security techniques - Codes of practice for information security management.* Geneva: International Organization for Standardization.

ISO/IEC 27005. (2011). *Information technology - Security techniques - Information security risk management.* Geneva: International Organization of Standardization.

ISO/IEC 31000. (2009). *Risk management - Principles and guidelines.* Geneva: International Organization of Standardization.

ISO/IEC TR 13335-2. (1997). *Information technology - Guidelines for the management of IT Security - Part 2: Managing and planning IT Security* (1st ed.). Geneva, Switzerland: ISO/IEC .

IT Governance Institute. (2000). *COBIT 3rd Edition.* Retrieved February 28, 2011, from IT Governance Institute: http://www.netbotz.com/library/Cobit_regulations.pdf

IT Governance Institute. (2007). *COBIT 4.1.* USA: IT Governance Institute.

Jochem, A., Bewier, A., Bongers, L., Borger, L., Coenen, H., Elsinga, B., et al. (2006, September). Security principles: Information security on the management agenda. *GvIB Expert Letter*. Netherlands: Genootschap van Informatie Beveiligers.

Jochem, A., Bongers, L., Coenen, H., Elsinga, B., Jonkman, E., Kuiper, R., et al. (2006, September). Seurity Principles: Information Security on the Management Agenda. *GvIB Expert Letter, 3*. GvIB.

Killmeyer, J. (2006). *Information security architecture: An integrated approach to security in the organization.* Boca Raton, FL: Auerbach Publications.

Kissel, R., Stine, K., Scholl, M., Rossman, H., Fahlsing, J., & Gulick, J. (2008). *Security Considerations in the System Development Life Cycle.* Gaithersburg: National Institutes of Standards and Technology.

Knowledge@ W.P Carey. (2008). *Business Ethics: College Cheating Is Bad for Business.* Retrieved August 2, 2011, from Knowledge @ W.P Carey: http://knowledge.wpcarey.asu.edu/article.cfm?articleid=1679

Krippendorff, K. (2004). *Content Analysis: An introduction to its methodology 2nd Edition.* California, USA: Sage Publications, Inc.

Kritzinger, E., & Smith, E. (2008, October). Information security management: An information security retrieval and awareness model for industry. *Computers & Security, 27*(5 - 6), 224 - 231.

Kumar, R. (2005). *Research Methodology 2nd Edition.* New Delhi, London Oaks: Sage Publications.

Lainhart IV, J. W. (2000). COBIT ™ : A Methodology for Managing and Controlling Information and Information Technology Risks and Vulnerabilities. *Journal of Information Systems, 14*(s-1), 21-25.

Lapakko, D. (2009). *Argumentation: Critical thinking in action.* New York, USA: iUniverse.

Lethbridge, T. C., & Laganiere, R. (2005). *Object-oriented software engineering: Practical Software Development using UML and Java* (2nd ed.). Berkshire, England: McGraw-Hill-Education.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry.* Beverly Hills, CA: Sage Publications.

McCumber, J. (2005). *Assessing and managing security risk in IT systems: A structured methodology.* Boca Raton, FL: Auerbach Publications.

Minister of Education. (1997, November 26). Higher education act, 1997. Department of Education.

Ministry of Education. (2001, February). National plan for higher education. South Africa: Department of Education.

Mohamedbhai, G. (2015, January 09). *What role for higher education in sustainable development?* Retrieved August 28, 2015, from University World News: Global Window on Higher Education: http://www.universityworldnews.com/article.php?story=20150108194231213

Nalavade, K., & Meshram, B. (2011). Layered Security Framework for Intrution Prevention. *IJCSNS International Journal of Computer Science and Network Security, 11(6)*.

NIST. (1996). *Generally Accepted Principles and Practices for Securing Information Technology Systems.* USA: U.S. Department of Commerce.

NIST. (2007, July 3). *Computer Security Division: Computer Security Resource Center*. Retrieved June 13, 2012, from NIST National Institute of Standards and Technology: Information Technology Laboratory: http://csrc.nist.gov/publications/PubsSPs.html

NIST SP 800-30 . (2002). *Risk management guide for information technology systems.* Washington: U.S. Department of Commerce.

NIST SP 800-39. (2011). *Managing information security risk.* Washington, USA: U.S. Department of Commerce.

NIST SP 800-50. (2003). *Building an information technology security awareness and training program.* Washington, USA: U.S. Department of Commerce.

NIST SP 800-53 Rev 3. (2009). *Recommended security controls for federal information systems and organizations.* Washington, USA: U.S. Department of Commerce.

NIST SP 800-64 . (2008). *Security Considerations in the System Development Life Cycle (Special Publication 800-64 Revision 2).* Washington: U.S. Department of Commerce.

NMMU. (2008). Retrieved March 8, 2011, from Nelson Mandela Metropolitan University: http://portal.nmmu.ac.za/default.asp?id=71&sp=0&bhcp=1

NMMU. (2011). *General Prospectus.* Retrieved July 27, 2011, from Nelson Mandel Metropolitan University: http://my.nmmu.ac.za/documents/prospectus/2011_General_Prospectus.pdf

Noor, M. (2008). Case Study: A Strategic Research Methodology. *American Journal of Applied Science, 5(11)*, 1602-1604.

NSTISSI 4011. (1994). *National Security Telecommunications and Information Systems Security: National Training Standard for Information Systems Security Proffessionals.* Fort George G. Meade: National Security Agency.

NUI. (2007). *The Academic Quality Assurance Programme 2005-2006: Review of Examinations Office.* Retrieved July 27, 2011, from National University of Ireland: hppt://www.nuigalway.ie/quality/downloads/examsudarasrep06final.pdf

Oates, B. (2006). *Researching information systems and computing .* London: Sage Publications.

Olivier, M. S. (2004). *Information Technology Research: A practical guide for computer science and informatics.* Pretoria: Van Schaik Publishers.

Ospina, S. (2003). *Quality Research.* Retrieved June 6, 2011, from Encyclopedia: http://wagner.nyu.edu/leadership/publications/files/Qualitative_Research.pdf

Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. (2010). *Human factors and information security: Induvidual, cultural and security environment.* Edinburgh, Australia: Australian Government Department of Defence.

Patterson, T. (2003). Holistic security: Why doing more can cost you less and lower your risk. *Computer Fraud & Security, 2003*(6), 13-15.

Pavlov, G., & Karakaneva, J. (2011). Information Security Management System in Organization. *Trakia Journal of Sciences, 9*(4), 20-25.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2008). A design science research methodology doe information systems research. *Management Information Systems, 24*(3), 45-78.

Posey, C., Roberts, T. L., & Courtney, J. F. (2011). *A Best Practices Guide to Information Security.* Washington: IBM Center for The Business of Government.

Posthumus, S., & von Solms, R. (2004). A framework for the governance of information security. *Computers & Security*, 638-646.

Quality Assurance Agency for Higher Education. (2006). *Code of practice for the assurance of academic quality & standards in higher education.* Mansfield: Linney Direct.

Reddy, G., Srinivasu, R., Rikkula, S. R., & Rao, V. S. (2009). Management Information System to help managers for providing decision making in an organization . *International Journal of Reviews in Computing, 5*(1), 1-6.

Ross, A. M. (1973, February). The role of higher education institutions in national development. *JSTOR, 2*(1), 103-108.

SANS Institute (2002). *An overview of threats & risk assessment.* Retrieved March 11, 2013, from SANS Institute InfoSec Reading Room: http://www.sans.org/reading-room/whitepapers/auditing/overview-threat-risk-assessment-76

SASCO. (2009). Debating institutional autonomy and academic freedom: search for a perspective. *SASCO 2009 16th National Congress.*

Sasse, M. A., Brostoff, S., & Weirich, D. (2001, July). Transforming the 'weakest link' - a human/computer interaction approach to usable and effective security. *BT Technology Journal, 19*(3), 122-131.

Saunders , M., Lewis , P., & Thornhill, A. (2007). *Research methods for business students.* Harlow: Financial Times Prentice Hall.

Schweitzer, J. A. (1982). *Managing information security: A program for the electronic information age.* Boston, USA: Butterworth (Publishers) Inc.

Shapiro, H. T. (2005). *A larger sense of purpose: Higher education and society .* Princeton: Princeton University Press.

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

Stefanek, G. L. (2002). *Information security best practices: 205 Besic rules.* USA: Butterworth-Heinemann.

Stroie, E. R., & Rusu, A. C. (2011). Security risk management - Approaches & methodology. *Informatica Economica, 15*(1).

Sutherland-Smith, W. (2008). *Plagiarism the Internet & student learning: Improving academic integrity.* New York: Routledge.

Taylor-Powel, E., & Steele, S. (1996). *Collecting Evaluation Data: Direct Observation.* Retrieved June 8, 2011, from http://learningstore.uwex.edu/assets/pdfs/G3658-5.pdf.

Thomson, M. E., & Von Solms, R. (1998). Information security awareness: Educating your users effectively. *Information Management & Computer Security, 6*(4(1998)), 167-174.

Tipton, H. F., & Krause, M. (2008). *Information security management handbook* (Sixth ed.). Boca Raton, FL, USA: Auerbach Publications.

Todd, J. (2007). *What is the impact of new technology in the workplace*. Retrieved November 6, 2011, from Helium: http://www.helium.com/items/436615-what-is-the-impact-of-new-technology-in-the-workplace

Tomhave, B. L. (2005). Alphabet Soup: Making Sense of Models, Frameworks, and Methodologies.

Tuller, C., & Oblinger, D. (n.d.). *Information Technology as a Transformation Agent.* Retrieved August 10, 2011, from Educause: http://net.educause.edu/ir/library/html/cem/cem97/cem9746.html

United States General Accounting Office. (1999). *Information security risk assessment.* Retrieved Feb 20, 2013, from GAO: US Government Accountability Office: http://www.gao.gov/products/AIMD-00-33

University of East London. (n.d). *Assessment & Feedback Policy.* Retrieved August 13, 2013, from UEL: http://www.uel.ac.uk/qa/policies/assessmentpolicy/

University of Toronto. (2009). *Academic Integrity Handbook: Preventing and Resolving Allegations of Academic Misconduct.* Retrieved August 12, 2011, from http://home.psych.utoronto.ca/Assets/Psych+Digital+Assets/Resources+for+Instructors/academic_handbookII.pdf

Vacca, J. A. (2010). *Managing information security.* USA: Elsevier.

Von Solms, B. (2001). Information Security - A multidimensional discipline . *Computers & Security*, 504-508.

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security, 23*(2004), 371-376.

Von Solms, R. (1999). Information security management: Why standards are importatnt. *Information Management & Computer Security, 7*(1), 50-57.

Von Solms, S. H. (2005). Information Security Governance - Compliance management vs operational management. *Computers & Security, 24*, 443-447.

Von Solms, S. H., & Von Solms, R. (2009). *Information security governance.* New York, USA: Springer Science + Business Media.

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

WBI Evaluation Group. (2007). *Guided expert reviews: Needs assessment knowledge base.* Retrieved 08 13, 2013, from World Banks Group Internet: http://www.siteresources.worldbank.org

White, M. (2010). *Research Methods 8th Edition.* Belmont, USA: Wadsworth Cengege Learning.

Whitman, E. M., & Mattord, H. J. (2008). *Management Information Security 2nd Edition.* Boston, USA: Course Technology Cengege Learning.

Whitman, M. E. (2004). In defense of the realm: understanding the threats to information security. *International Journal of Information Management, 24*, 43-57.

Whitman, M. E., & Mattord, H. J. (2003). *Principles of information security .* Canada: Course Technology.

Wilkinson, P., & Schilt, J. (2008). *ABC of ICT: An Introduction.* Zaltbommel: Van Haren Publishing.

Wuensch, K. L. (2011). *Sampling.* Retrieved 11 25, 2013, from http://www.core.ecu.edu

Yin, R. K. (2003). *Case study research: Design and methods* (3rd ed.). Thousand Oaks: Sage Publications.

York University. (2007). *Policies, Procedures, And Regulations: Conduct of Examinations, Policy & Guidelines on the.* Retrieved July 27, 2011, from York

University:

http://www.yorku.ca/univsec/policies/document.php?document=808plain=y

APPENDICES

Appendix A - ISSA Conference Paper 2014

Information Security Assurance Model (ISAM) for an Examination Paper Preparation Process

Miemie Mogale[1], Mariana Gerber[2], Mariana Carroll and Rossouw von Solms
School of Information and Communication Technology
Nelson Mandela Metropolitan University
Port Elizabeth, South Africa
[1]miemie.mogale@gmail.com
[2]mariana.gerber@nmmu.ac.za

Abstract— **Information and Communications Technology (ICT) has infiltrated Higher Education Institutions (HEIs), and HEIs' processes, such as the Examination Paper Preparation Process (EPPP). The EPPP too have become reliant on ICT for the processing, storage and transmission of examination papers. The use of ICT in the EPPP has made it convenient for examiners to prepare and collaborate on examination papers; however, ICT is continuously exposed to a wide range of threats and vulnerabilities, which could compromise the security of the examination papers, if not addressed. These threats and vulnerabilities include examiners' negligent behaviors while preparing the examination papers. Examples of these include: not encrypting stored or transmitted examination papers, which could be intercepted by hackers; leaving computers unlocked and unattended while working on examination papers. Such contraventions in the EPPP may lead to some students being conferred with qualifications that they do not deserve.**

This paper has critically assessed a HEI's EPPP to identify threats and vulnerabilities that could place the security of the process at a risk. Surveys were utilized to identify certain examiner behaviour which could pose as risk to the security of the examination papers. The paper further highlights the vital role the human factor plays in ensuring that the EPPP is secure.

The paper proposes an Information Security Assurance Model (ISAM) that is based on information security principles and best practices to manage and improve the security of the EPPP. The model provides a step-by-step guide which could be followed to ensure that relevant information security aspects are considered to ensure that examination papers are handled more securely.

Keywords— higher education institutions; information and communications technology; information security; information security management system; information security risk management; threats; vulnerabilities

I. Introduction

With the expansion of Information and Communication Technology (ICT), new technologies have become available to facilitate the use and dissemination of information (Todd, 2007). As with most organizations ICT has infiltrated Higher Education Institutions (HEIs). It has become the primary vehicle for the processing, storage and transmission of various institutions' vital information. ICT has made it convenient for HEIs' employees to collaborate on projects and share information without the limitations of geographical boundaries.

The ubiquitous of ICT has contributed significantly in HEIs, as it has various uses. Amongst the many uses, ICT is used as a teaching and learning mechanism; as well as used for institutions' preparation of examination papers. The process of preparing examination papers is referred to as the Examination Paper Preparation Process (EPPP). The EPPP is the process that ensures that examination papers are set and ready for the examination to take place. The process ensures that the papers are compiled (set), moderated and authorized on time, before the papers are submitted to the Examinations Office to be duplicated and kept securely until the date of the examinations.

With ICT, examiners are able to work on examination papers from anywhere and can collaborate with another examiner on an examination paper. Examiners use computers and laptops to compile their examination papers. They then use mobile storage devices to store the examination papers for later retrieval, backup purposes or to work from home. Communication methods such as emails are used to transmit the examination papers amongst each other when collaborating on the examination papers, as well as to transmit to moderators for moderation and HODs for authorization. The use of ICT assists all role players in the process of preparing the examination papers in an efficient and productive manner, in order to be complete and ready on time for the examination to be written. Although ICT has made it more convenient to prepare examination papers, it also has its drawbacks. ICT is continuously exposed to a wide range of threats, which may compromise the security of the examination papers, which may, undermine the integrity of the EPPP. The problem is escalated further by individuals whom may lack security considerations when handling examination papers, either through the use of ICT or manually, causing their practices to potentially compromise the security of the examination papers.

The aim of this paper is to propose an information security assurance model, which aims at highlighting the importance of knowing the threats and vulnerabilities faced by information security as the best way of formulating an information security defence. Further highlighted, is the vital role the human factor plays in ensuring that examination papers are secure while being prepared. The paper critically assesses a HEI's EPPP and identifies certain role players' behaviour which could pose as risk to the security of the examination papers.

The remainder of the paper will be as follows: Section II provides the background into HEIs and the EPPP. Section III discusses an information security management system as means of managing and improving the security of a process. Section IV follows with the research methodology followed. Section V is the proposed model conception and development, which is followed by section VI, the solution - the Information Security Assurance Model (ISAM). The paper concludes in section VII.

II. BACKGROUND

Higher Education Institutions (HEIs) are institutions that provide Higher Education (HE). HE plays a central role in the social, central and economic development of the nation. One of its goals being to ensure national growth and competitive edge; which is dependent on continuous technology improvement and innovation. HEIs are the vehicle through which the goals of HE are achieved. HEIs are responsible for creating and transmitting knowledge to students, as well as producing skills and knowledge that will meet the economic and social requirements of the nation. In order for HEIs to meet their responsibilities, they have to be accountable to the public, by producing knowledgeable graduates of high-quality skills and competencies. This can be part achieved by ensuring that qualifications are awarded to deserving students who have demonstrated the competence in the achievement of the learning outcome of a module. To gain evidence of the competence of students, HEIs rely primarily on examinations.

Examinations assess the knowledge of a student to give assurance that the student has sufficient understanding of that which is being assessed. For HEIs, examinations are a way of collecting evidence of a student's competence to demonstrate the achievement of the learning outcome of a module. For future employers they give assurance that the passing students have the basic understanding of the work and that they are competent.

But if students have access to examination papers before the examinations take place, what assurance is there for employers out there? If students cheat, it undermines the integrity of the HEIs and their examination process. In addition, it may cost the institution its credibility in the industry, especially if students keep passing and obtaining qualifications without demonstrating the required level of understanding and basic knowledge because of cheating. This not only undermines the integrity and credibility of the HEIs, it may also cost the institutions much needed funding from various donors. Therefore, HEIs should strive to ensure that academic dishonesty is prevented and detected.

It is the responsibility of HEIs to ensure that an effectively controlled and secure examination process is in place, to help safeguard reputational damage, as well as the hardworking students. This could be achieved by ensuring, in part, that the examination papers are not accessible to unauthorised persons. To exercise control, there needs to be a proper management system in place, one that takes into account the security of examination papers within the examination process. The management system needs to address the risks pertaining to the process; including the risks pertaining to the use of ICT for the processing, storage and transmission of the examination papers. Further, the management system needs to take into consideration the human factor within the process, and the vital role the human factor plays in ensuring that the examination papers are kept secure. This could be achieved by ensuring that an effectively controlled and managed EPPP is in place; one that safeguards the security of the examination papers, by addressing the risks and role players' behaviour and practices that could compromise the security of the examination papers.

The EPPP is the process of preparing examination papers; from the moment the papers are set by the respective examiners, to when the papers are submitted to the Examinations Office (for duplication and safe storage till the examinations are written). The process of an EPPP of a particular HEI is depicted in Figure 1.

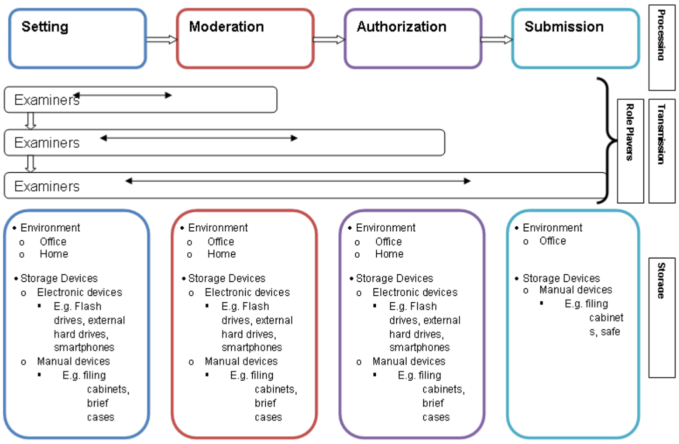


Fig 1. Examination Paper Preparation Process

For the purpose of this paper, the process involves the setting of the papers by the examiners; the storage of the papers during the time; the transmission of the papers amongst examiners (if collaborating on the paper), to transmission to internal moderators for moderation, as well as to the head of department (HOD) for authorization, and lastly, transmission to the Examinations Office.

The process is, thus, based on the:

- **Processing** of the examination papers, which is the four stages that the papers go through (setting, moderation, authorization and submission).
- **Transmission** of the papers, which illustrates the transmission of the papers amongst the various role players in the process (examiners, moderators, head of departments (HODs) and examinations officers).
- **Storage** of the papers, which depicts the various locations that the papers can be found, and the types of devices that the papers can be stored in.

Role players refer to all those individuals involved in the EPPP (examiners, internal moderators, HODs and examinations officers). Quite often, role players in the EPPP, while going about their daily activities during the process may lack security considerations when it comes to their practices. At times they might not be aware that their daily practices and behaviour could be potential vulnerabilities in the process. They are unaware that what they are doing could compromise the security of the examination papers and the entire EPPP. While performing their day-to-day activities, they may only be thinking of getting the examination papers completed on time, without being conscious of any security related issues, especially with the use of ICT. However, without being aware of their unconscious negligent practices and without taking security into consideration, this could lead to a serious security breach, thus, placing the examination papers and the process in jeopardy and at risk. The security of the examination papers could be compromised by overlooking just a single vulnerability that may be exploited by a threat. It is thus imperative that all role players be aware of their unconscious negligent behaviour in order to ensure that the examination papers are well protected during the process and while using ICT.

The following section (section III) discusses an information security management system as means to assist in ensuring an effectively controlled and managed EPPP, which manages and improve the security of the examination papers.

III. INFORMATION SECURITY MANAGEMENT SYSTEM

ICT along with the Internet have provided convenient ways of storing information and of transporting information to other remote locations. Electronic methods, such as emails, on-line storage (i.e. dropbox, google apps amongst others) are being used by a growing number of employees to transmit and distribute or make available documents amongst each other. However, the use of ICT, along with the Internet, has also increased the incidents of information abuse or misuse. People are now able to access information remotely, where detection can go unnoticed, as well as remove valuable information, using mobile storage devices (Dhillon & Backhouse, 2000). Furthermore, the use of ICT and the Internet has increased and introduced a new range of threats and vulnerabilities facing information, thus, putting the information at an even greater risk (Whitman, 2004).

When dealing with the risks, many researchers suggest managing the risks through the implementation of a proper and comprehensive information security management system (ISMS) (Eloff & Eloff, 2003; Pavlov & Karakaneva, 2011). In addition, the ISMS needs to pay attention to the human factor in the organization, and the role that the human factor plays in effectively protecting information (Posthumus & von Solms, 2004). The reason being; it is people who handle and work with the organization's information on a daily basis, and these people often do so negligently and in an insecure manner.

An ISMS can be defined as 'Coordinated activities to direct and control the preservation of confidentiality, integrity, and availability of information' (Tipton & Krause, 2008). Eloff and Eloff (2003), further define an ISMS as a management system used for establishing and maintaining a secure information environment.

Thus, an ISMS can assist organizations in managing information security in a holistic manner, which will assist in addressing all relevant information security aspects that deal with creating and maintaining a secure information environment. According to von Solms (2001), information security aspects are considered to be security controls or best practices, which need to be considered in order to create a secure information environment. These information security aspects include: organizational structure; policy; best practices; risk assessment; awareness, education, and training; human factor; and compliance, amongst others (Von Solms, 2001; Von Solms & Von Solms, 2004; Killmeyer, 2006). A brief discussion on these aspects follows:

- Organizational structure deals with "the way information security is organized and structured in an organization" (Von Solms B., 2001). For information security efforts to be successful, information security has to be properly managed and coordinated within the organization.
- Information security policy is a direction-giving document for information security within an organization, providing management direction and support for information security. It is also a mandate and reference framework for the effective implementation of the other information security controls (Hone & Eloff, 2002; NIST SP 800-53 Rev 3, 2009). The policy dictates acceptable user behavior when handling organization's information assets and when using the ICT systems that process, store and transmit the information assets.
- Best practices, also referred to as good practices, are "proven activities or processes that have been successfully used by multiple organizations" (ISACA, 2012). These are tried and tested practices that if followed may help address most information security risks, and assist in ensuring that all information security bases are covered (Von Solms B., 2001).
- Risk assessment is essential for the identification and evaluation of risks pertaining to a particular environment, or the use of ICT systems for the processing, storage and transmission of valuable information. The results of the risk assessment can thereafter help guide and determine appropriate actions and security controls, for the mitigation and management of the risks (NIST SP 800-30, 2002; ISO/IEC 27002, 2005).
- Human factor deals with the behavior and practices of authorized individuals who have access to the organizations information assets and the ICT systems that process, store and transmit the information (ISO/IEC 27002, 2005; NIST SP 800-53 Rev 3, 2009).
- Awareness, education and training is about ensuring that all information users are aware of and educated regarding information security in the organization, as well as trained. Awareness is about informing information users of threats and vulnerabilities that could compromise the security of information assets (ISO/IEC 27002, 2005; Von Solms B., 2001; NIST SP 800-50, 2003). Organizations can have the best information security programs, with the best technical security controls, as well as well written information security policies and procedures; however, without information users being aware of those, then they do not serve any purpose.
- Compliance relates to both legislative compliance and information security policy compliance. It is ensuring that appropriate security controls are in place in order to avoid breaches of any legal form such as law, regulation or contractual obligation (ISO/IEC 27001, 2005).

The discussed information security aspects have been identified as relevant aspects to be considered in order to create a secure EPPP. These aspects will ensure that the information security effort addresses all relevant information security issues and concerns of the EPPP. In an effort to create a secure EPPP, a model is proposed, which adopts the characteristics of an ISMS, by taking into consideration the identified information security aspects. With the adoption of the PDCA model, the aspects will be coordinated.

Before discussing the proposed model, the next section (section IV) discusses the methodology followed to identify certain role players' behaviors that could compromise the security of the examination papers, thus placing the EPPP at risk.

IV. RESEARCH METHODOLOGY

A qualitative approach was followed and a case study strategy applied for the research of this paper. According to Anderson (1998), a qualitative approach, is a form of inquiry that explores phenomena in their natural setting and uses multi-methods to interpret, understand, explain and bring meaning to them. In the case of this paper, the role players' practices while preparing examination papers were explored in order to interpret their practices and obtain an understanding in regards to information security.

A case study strategy was applied in conducting this research study. A case study is a holistic research strategy that uses multiple sources of evidence to analyse or evaluate a specific phenomenon (Anderson, 1998, p152). For this paper a case study was applied to enquire about role players' practices when preparing examination papers at a particular HEI, in terms of compiling, storing and transmitting the examination papers. Further investigated was the documented examination policy and procedures document.

Anderson (1998), further states that a case study is concerned with how and why things happen, allowing the investigation of contextual realities and the differences between what was planned and what actually occurred.

This paper investigated how examiners and moderators prepared and moderated the examination papers. It investigated their practices when compiling/moderating, storing and transmitting the examination papers. It further investigated, through observation, how the examinations officers accepted the examination papers from the examiners. This was then compared to what is expected, based on the documented examination policy and procedures, in order to identify the actual practices versus the documented expected practices. This also assisted in identifying the shortfalls of the documented policy regarding what is expected of role players.

The data collection methods employed were as follows:

- Literature review – literature on HEIs, the examination process, information security, ISMS and information security best practices.
- Interviews – interviews were conducted with: the Deputy Director of Examinations; a few selected examiners (who some are also internal moderators); and examinations officers. The interviews were conducted to gain insight on the examination process, and on what the EPPP entails.
- Questionnaires – the questionnaires were distributed to randomly selected examiners (who some were also internal moderators) to elicit information about their practices and the ICT resources they use to process, store and transmit the examination papers when preparing them. Some of the questions which were asked were: which mobile devices they used when preparing examination papers; if they had left office doors and computers screens opened and unattended; if they had found examination papers left on shared printers; if they encrypt stored or emailed examination papers; if they are aware and have read the examinations policy and procedure documents just to name a few.
- Observation – the author spent some time in the Examinations Office, in order to observe the general security of the environment and how the examination papers are handled in the Examinations Office. Furthermore, it was to observe the examiners when they brought in their examinations papers, to establish if they followed what the documented policy stated regarding the bringing in of examinations papers.
- Document review – a qualitative content analysis was conducted which assisted in the interpretation of the contents of the examination process policy and documented procedures in order to understand and bring meaning to the contents of the documents. This assisted in gaining insight of how the examination process is expected to be, in particular the EPPP, especially pertaining to the security of examination papers and what role players are expected to do.

V. RESEARCH RESULTS

From the interviews with the Deputy Director of Examinations and a few selected examiners, insight was gained on what the EPPP entails and what methods are used for the transmission and storage of examination papers (as depicted in Figure 1). From the questionnaires, the following were revealed:

- Some examiners have left office doors and computer screens opened and unattended, which makes it easy for someone to gain access to what is stored on the computer, including an examination papers
- Most never encrypt the stored or transmitted examination papers.
- Some revealed that they have thrown draft examination papers in dustbins without shredding them.
- Others do not have anti-virus software installed on their computers and some of those who have, have never updated it.
- Most were not aware and have never read the examination policy and procedures document;

therefore, they are not aware of what is expected of them.

- The document review revealed that that security is not explicitly stressed in the policy. The policy only mentioned that the examination papers should be at all times encrypted.

From the documents reviewed, it was revealed that security was not addressed adequately. The only requirement that was mentioned is that papers should be encrypted, but nothing was mentioned on the other security concerns; such as ensuring that screens are locked at all times if not attended, and locking of office doors, as well as properly discarding drafts, to mention but a few.

From the observation, the author observed that from the Examinations Office side papers were handles securely. Entrance to the office is limited to the examinations stuff through a finger print biometrics access control. Once examinations officers accept examination papers, they place the examination papers in the safe, when they are not busy with it. However, when it came to examiners submitting the papers, it was observed that some of the examiners did not follow the procedure as documented in the policy. They would bring the papers with out placing them in folders as documented. This could compromise the security of the paper, as the paper may fall without being notices, especially since the examiner would sometimes be carrying other documents as well. During the observation, examiners were asked if they were aware of the examinations policy, and some were not, therefore, it could be deduced that they had no idea of what is expected of them, as documented in the policy.

Thus, from this information, it could be deduced that the examination papers could be compromised due to the role players' negligent behavior and practices when handling examination papers, as well as the lack of security being mentioned in the policy document.

As a result, this paper proposes an information security model that will assist in managing and improving the security of the EPPP; model which will ensure that the risks pertaining to the process are addressed as well as the human factor.

The following section (section VI) discusses the proposed model.

VI. INFORMATION SECURITY ASSURANCE MODEL (ISAM)

The aim of the proposed model is to manage and improve the security of the examination papers handled during the EPPP, by ensuring that all possible risks pertaining to the EPPP are accounted for. The model aims to provide the examinations management team, responsible for setting the EPPP, with all the necessary steps and guidance required to ensure reasonable assurance that the examination papers are secure, thereby, improving the security of the EPPP. The word "assurance" does not imply total guarantee of security, because one can only aim for reasonable security, since security can never be totally guaranteed. Therefore, in the proposed model "assurance" refers to the intent to give confidence that due care and due diligence has been performed to ensure that all necessary steps have been taken, in order for the examination papers to be secure.

The **ISAM** (depicted in Figure 2) is a management system, which aims to manage and improve the security of the EPPP.

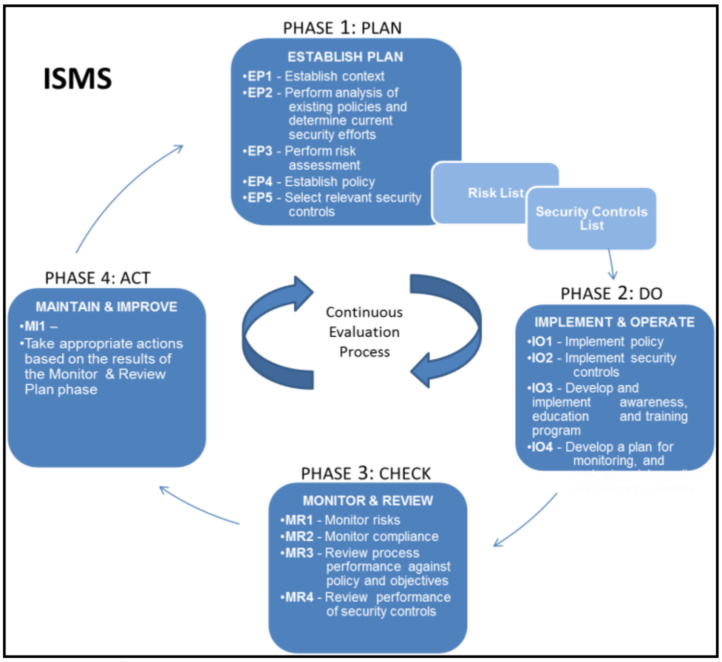

ISMS
PHASE 1: PLAN
ESTABLISH PLAN
•EP1 - Establish context
•EP2 - Perform analysis of existing policies and determine current security efforts
•EP3 - Perform risk assessment
•EP4 - Establish policy
•EP5 - Select relevant security controls
Risk List
Security Controls List
PHASE 2: DO
IMPLEMENT & OPERATE
•IO1 - Implement policy
•IO2 - Implement security controls
•IO3 - Develop and implement awareness, education and training program
•IO4 - Develop a plan for monitoring, and
PHASE 3: CHECK
MONITOR & REVIEW
•MR1 - Monitor risks
•MR2 - Monitor compliance
•MR3 - Review process performance against policy and objectives
•MR4 - Review performance of security controls
PHASE 4: ACT
MAINTAIN & IMPROVE
•MI1 –
•Take appropriate actions based on the results of the Monitor & Review Plan phase
Continuous Evaluation Process

Fig 2. Information Security Assurance Model

The model is informed by the **ISMS:** a management system for establishing and maintaining a secure environment; and designed to ensure the selection of adequate and appropriate security controls that protect information assets and satisfy and meet the identified information security requirements of a particular environment. The model will ensure that adequate and appropriate security controls are selected, and that the selection is based on the results of a risk assessment.

The model is a guiding process which consists of various activities, which need to be performed, in order to secure the examination papers. These activities are related to four **Information Security Aspects**, which were identified as relevant for the EPPP, for creating a secure information environment. The aspects assists in ensuring that relevant concepts will not be overlooked, but considered and addressed, in order to manage and improve the security of the EPPP, and ensure that examination papers are adequately and appropriately protected. The four aspects are: **Policy; Risk Assessment; Awareness, education and training; and Compliance**. These aspects are not explicitly presented in the model; however, the activities related to these aspects are presented.

The model adopts the **PDCA model** to help structure all the model activities. The model further consists of two additional guiding lists: **Risk List and Security Controls List**. The information security best practices are explicit in the **Security Control List**. **The Security List** provides a list of possible security controls, identified from ISO 27002 (2005) and NIST SP800-51 Rev1 (2006). The security controls were identified based on the identified risks, and understood as appropriate controls for the mitigation of the risks. The identified risks are presented in the **Risk List** of the proposed model. The **Risk List** was influenced by the information security principle of securing information from a risk approach, which means the securing of information is based on identified risks.

The ISAM further comes with an addendum: **ISAM Detailed Guide,** which provides detailed guidance for the implementation of each of the phases of the ISAM.

The following section (section VII), discussed the various components of the model in detail (the four phases, the Risk List, Security Controls List as well as the ISAM Detailed Guide).

VII. ISAM COMPONENTS AND GUIDES

The ISAM consists of four phases: Establish Plan, Implement & Operate, Monitor & Review, and Maintain & Improve. Each phase in turn, consists of a number of activities, numbered: EP1-EP5; IO1-IO3; MR1-MR4; MI1, as listed below in Table 1 Phases. These activities are the actions that need to be carried out in order to create a secure EPPP that preserves the confidentiality, integrity and availability of the examination papers. To help structure the activities, the model adopted the PDCA model, as mentioned in section VI, and presented in Figure 2.

Further presented in the ISAM are three additional guides, namely the Risk List, the Security Controls List and the ISAM Detailed Guide.

Risk List

The Risk List is included in the model as additional guide that can be used by the examinations management team to identify similar risks and to support a risk assessment effort performed by the management team. The Risk List was compiled from the assessment of the EPPP of a particular higher education institution (HEI), where certain risks were identified pertaining to the process. Risks are caused by threats taking advantage of known/unknown vulnerabilities, compromising assets, resulting in an adverse impact. Therefore, risk is the result of the relationship between an asset, threat and vulnerability. Table II illustrates a sample list of identified risks. The risks listed are potential risks that could exist in any similar process environment.

TABLE I. PHASES

Phase 1: Plan - Establish Plan (this phase establishes the plan; by identifying the objectives and determining the context) *The phase consists of* ***five activities***: EP1 - Establish context EP2 - Perform analysis of existing policies and determine current security efforts EP3 - Perform risk assessment EP4 - Establish policy EP5 - Select relevant security controls	**Phase 2: Do - Implement & Operate Plan** (this phase ensures that the plan is implemented and operates as intended; in order to achieve the objectives identified in the plan stage) *The phase consists of* ***three activities:*** IO1 - Implement policy IO2 - Implement security controls IO3 - Develop awareness, education and training program
Phase 3: Check - Monitor & Review Plan (this phase ensures that all that has been implemented is reviewed to ensure that it is effective. This phase includes monitoring of changes) *The phase consists of* ***four activities:*** MR1 - Monitor risks MR2 - Review process performance against policy and objectives MR3 - Review performance of security controls MR4 – Monitor compliance	**Phase 4: Act - Maintain & Improve Plan** (this phase ensures that appropriate actions are taken based on the monitoring and reviewing) *The phase consists of* ***one activity:*** MI1 - Take appropriate actions based on the results of the Monitor & Review phase Further presented in the ISAM are the two additional guides: Risk List and Security Controls List

TABLE II. RISK LIST

ITEM NO.	**THREAT-SOURCE/VULNERABILITY**	**IMPACT**
IR1	Hacker/unencrypting	Unauthorized access can be gained to unencrypted examination papers while on storage or intercepted email communication.
IR2	Hacker/ineffective password communication	Unauthorized access to passwords can be gained through intercepted email communication or sent messages on lost mobile phones, resulting to unauthorized access to examination papers.
IR3	Hacker/open shares	Unauthorized access to stored examination papers gained through open shares.
IR4	Viruses & worms/no antivirus	Viruses or worms, through infected emails for instance, can corrupt the examination papers, or destroy a storage device, or cause a denial of service. Papers may even be altered due to viruses.
IR5	Viruses & worms/not updating antivirus	Not updating the antivirus software could cause the antivirus to be ineffective in detecting viruses, thereby, causing the corruption of examination papers, or destruction of storage devices, or denial of service, as well as altered papers.

The Risk List is presented in a table form, with three columns (**Item No., Threat-source/Vulnerability, and Impact**). The **Item No.** is a unique number representing each identified risk e.g. IR3. The **Threat-source/Vulnerability** represents a potential threat-source exploiting an identified vulnerability e.g. Hacker/open shares (a hacker exploiting an open share to gain access to information). The **Impact** represents the results of a threat-source exploiting a vulnerability e.g. unauthorized access to stored examination papers gained through open shares.

Security Controls List

The Security Controls List is included in the proposed model as an additional guide, which could be used by the examinations management team, to identify security controls that may be implemented to protect the examinations papers and improve security of the EPPP. A sample of security controls included in the Security Controls List is displayed in Table III.

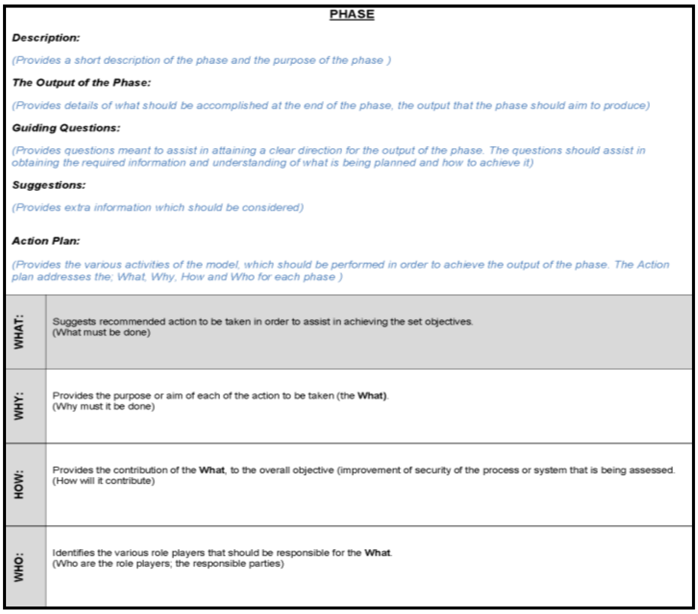
The Security Controls List presents a list of security controls, identified from the ISO 27002:2005 and NIST SP-53 Rev 1 (2006) standards, for the mitigation of the identified risks presented in Table 1's Risk List. The numbering contained in the last two columns of Table III (ISO27002 and NIST SP-53 Rev 1 columns), conforms to the numbering scheme of the various security controls in the two standards, respectively.

TABLE III. SECURITY CONTROLS LIST

SECURITY CONTROLS CATALOG		**ISO27002**	**NIST SP-53 REV 1**
Access Control	(Control access to information, by ensuring that only authorized persons have	11.1.1	AC-3
		11.2	AC-2
		11.5.1	AC-7
		11.5.5	AC-11
		11.4.4	AC-17

ISAM Detailed Guide

The ISAM Detailed Guide provides detailed guidance for the implementation of each of the phases of the ISAM. It is a step-by-step guide, which could be followed by the examinations management team to create a secure EPPP that protects the security of the examination papers. The ISAM Detailed Guide is intended to be generic, which can be adapted with minimal effort to similar environment or other HEIs, with the aim to ensure the security of valuable information asset, such as examination papers. By following the steps, a person using the model will be able to identify and select any process under consideration for assessment, and then follow the steps of the model to manage and improve the security of that specific process. Figure 3 provides a sample of the ISAM Detailed Guide as a template for illustrating how the guide is presented and structured in the model.



PHASE

Description:

(Provides a short description of the phase and the purpose of the phase)

The Output of the Phase:

(Provides details of what should be accomplished at the end of the phase, the output that the phase should aim to produce)

Guiding Questions:

(Provides questions meant to assist in attaining a clear direction for the output of the phase. The questions should assist in obtaining the required information and understanding of what is being planned and how to achieve it)

Suggestions:

(Provides extra information which should be considered)

Action Plan:

(Provides the various activities of the model, which should be performed in order to achieve the output of the phase. The Action plan addresses the; What, Why, How and Who for each phase)

WHAT:	Suggests recommended action to be taken in order to assist in achieving the set objectives. (What must be done)
WHY:	Provides the purpose or aim of each of the action to be taken (the **What**). (Why must it be done)
HOW:	Provides the contribution of the **What**, to the overall objective (improvement of security of the process or system that is being assessed. (How will it contribute)
WHO:	Identifies the various role players that should be responsible for the **What**. (Who are the role players; the responsible parties)

Figure 3: ISAM Detailed Guide Template

The ISAM Detailed Guide is applied to each of the four phases:

Establish Plan (Phase 1: Plan – Establish Plan): This is the first phase of the model. It is concerned with identifying the process to be assessed, and determining its scope and objectives. The phase should set the purpose and aim of the identified process, and define its objectives, in order to give direction on how the process should be. From there on, the process should be assessed, to determine any unwanted events that could deter the achievement of the objectives. Following should be the establishing of the policy and identifying and selection of relevant security controls.

Implement & Operate (Phase 2: Do - Implement & Operate): During the second phase the established policy and identified security controls are implemented and operated. Furthermore, an awareness, education, and training program is developed. The program is to ensure that all the role players of the process know what is expected of them in regards to performing their duties in a secure manner, as well as made aware of the risks pertaining to the process and means of safeguarding against those risks.

Monitor & Review (Phase 3: Check - Monitor & Review): The third phase is to ensure that the process is kept current and that risks are continually monitored as well as any changes known and documented. This phase involves reviewing the policy as well as the effectiveness and operation of implemented security controls, to ensure that those operate as intended. The phase also is concerned with ensuring compliance.

Maintain & Improve (Phase 4: Act - Maintain & Improve): The fourth phase is concerned with ensuring that the process is always maintained, and that it stays current. The phase involves taking actions to ensure that the results of the Monitor & Review phase are implemented.

By following the proposed model's guidance, the examinations management team could be assisted to show that due care and diligence was performed during decision-making, to ensure that adequate and appropriate controls are selected and implemented for the protection of the examination papers.

VIII. CONCLUSION

The proliferation of ICT caused many processes within organizations to be exposed to threats. The EPPP process within HEI's is no exception. With human involvement as role players in setting, managing, storing and transmitting of examination papers, the process is placed further at risk. Hence, the need for a secure EPPP was established.

The paper highlights the vital role that the human factor plays in ensuring that the EPPP is secure. By assessing the EPPP of a HEI, the threats and vulnerabilities that could place the security of the process at risk, were identified.

The paper proposes an Information Security Assurance Model (ISAM) that is based on information security principles and best practices to manage and improve the security of the EPPP. The model provides a step-by-step guide which could be followed in compiling a EPPP policy to ensure that relevant information security aspects are covered to contribute to more secure handling of examination papers.

References

Dhillon, G., & Backhouse, J. (2000, July). Information System Security Management in the New Millennium. *Communications of the ACM, 43*(7), 125-128.

Eloff, J., & Eloff, M. (2003). Information Security Management - A New Paradigm. *SAICSIT*, (pp. 130-136).

Hone, K., & Eloff, J. H. (2002, October 1). Information security policy - What do international information security standards say? *Computers & Security, 21*(5), 402-409.

ISACA. (2012). *COBIT 4.1: Framework for IT Governance and Control*. Retrieved June 6, 2012, from ISACA: http://www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx

ISO/IEC 27001. (2005). *Information technology - Security techniques - Information security management system - Requirements.* Geveva: International Organization of standardization.

ISO/IEC 27002. (2005). *Information technology - Security techniques - Codes of practice for information security management.* Geneva: International Organization for Standardization.

Killmeyer, J. (2006). *Information security architecture: An integrated approach to security in the organization.* Boca Raton, FL: Auerbach Publications.

NIST SP 800-30 . (2002). *Risk management guide for information technology systems.* Washington: U.S. Department of Commerce.

NIST SP 800-50. (2003). *Building an information technology security awareness and training program.* Washington, USA: U.S. Department of Commerce.

NIST SP 800-53 Rev 3. (2009). *Recommended security controls for federal information systems and organizations.* Washington, USA: U.S. Department of Commerce.

Pavlov, G., & Karakaneva, J. (2011). Information Security Management System in Organization. *Trakia Journal of Sciences, 9*(4), 20-25.

Posthumus, S., & von Solms, R. (2004). A framework for the governance of information security. *Computers & Security*, 638-646.

Tipton, H. F., & Krause, M. (2008). *Information security management handbook* (Sixth ed.). Boca Raton, FL, USA: Auerbach Publications.

Todd, J. (2007, July 4). *What is the impact of new technology in the workplace*. Retrieved November 6, 2011, from Helium: http://www.helium.com/items/436615-what-is-the-impact-of-new-technology-in-the-workplace

Von Solms, B. (2001). Information Security - A multidimensional discipline . *Computers & Security*, 504-508.

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*(23), 371-376.

Whitman, M. E. (2004). In defense of the realm: understanding the threats to information security. *International Journal of Information Management, 24*, 43-57.

Appendix B – Interview Guide: Deputy Director Examinations

INTERVIEW QUESTIONS

For the Head of Examinations

With the questions I'm trying to understand the examinations process and how the process of setting of examination papers fit in the process.

Further, it is to find out if any information security frameworks or best practices were considered when planning and developing the examination process.

The response will help in formulation the problem statement.

No.	INTERVIEW QUESTION	PURPOSE
1.	What is the main of the exam process?	To determine if they have considered the security aspect (protection of exam papers).
2.	What is the aim of the exam process?	To determine what they aimed to achieve by the way the process is set
3.	What does the process of setting examination papers entail?	To understand the process of setting examination papers
4.	What are the challenges that are currently facing the Examinations Office?	To determine any challenges facing the Examinations Office regarding the process
5	Is there any other issues raised by the auditors, which are a security concern?	To identify any security concerns
6.	Were there any framework that you followed for the process and the development of the exam process policy?	To find out if they had followed any set framework or it was all ad hoc.
7.	Did you use any person with an information background to help, or even follow any information security best practices?	To find our if they had considered the information security behind the whole process
8.	Are there any documented policy and procedures for the process of setting examination papers?	To find out what documentations are available
9.	How are the documentation communicated to the relevant people?	To determine the communication means for the policy
10.	How do you ensure that the relevant people follow the policy?	To determine if the are ways of determining if the relevant people know what is expected of them

QUESTIONS AND ANSWERS

INTERVIEWER: Researcher

INTERVIEWEE: Deputy Director of Examinations

DATE: 8/07/2011 8:30 -9:00

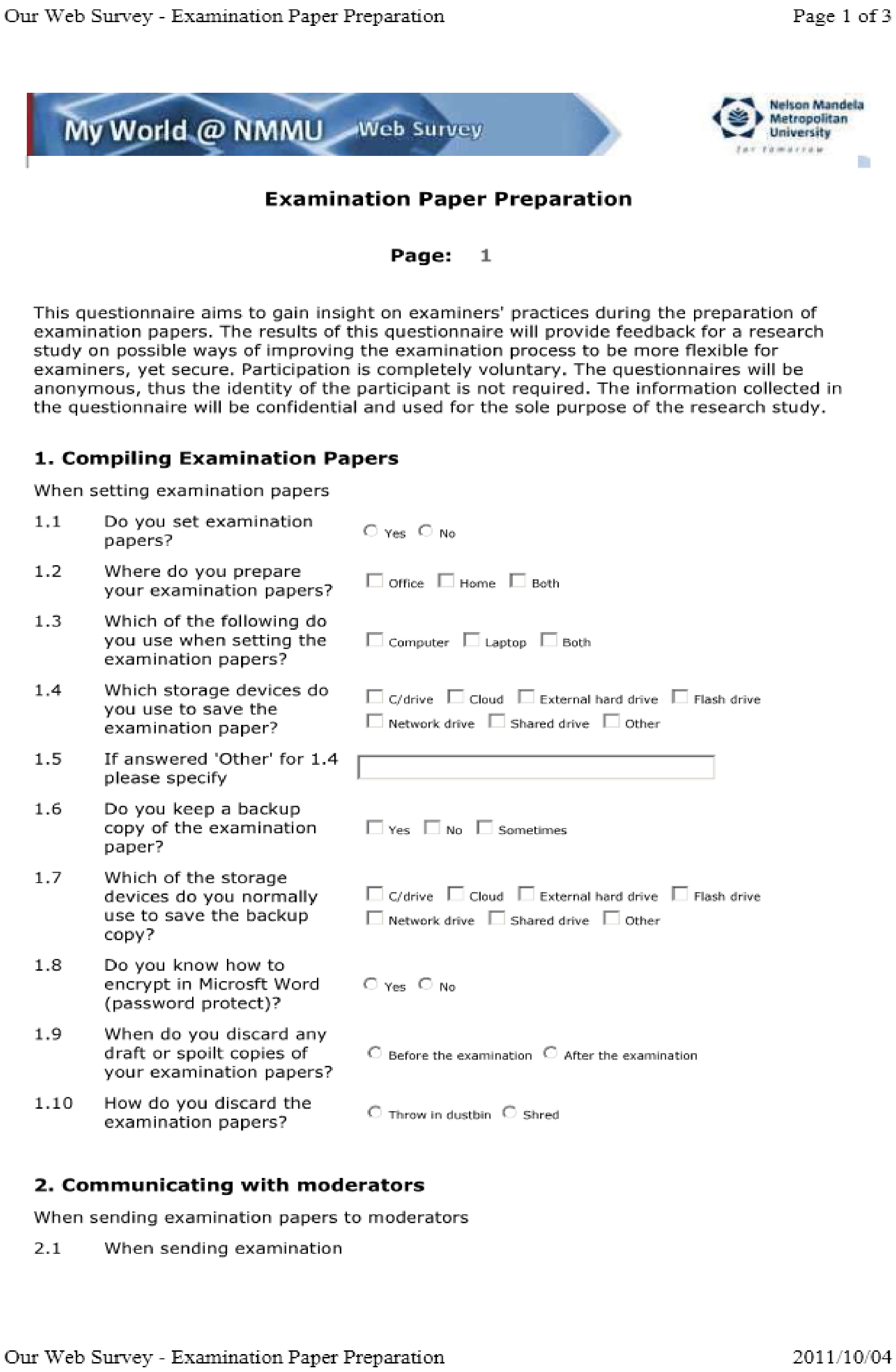
1. **What does the examination process entails?**
   Well the process is made up of different sub-processes. It involves: timetabling, which ensures that modules of a stream are sufficiently spread out for the student's convenience; booking of various examination venues according to the number of students per module; ensuring that examination papers are set and ready for examinations; ensuring that external moderators are appointed for all exit modules or any other modules that may require external moderation; appointment of external examiners if need be; appointment of invigilators for each examination. All the various sub-processes are performed at different intervals of the examination process.
2. **What is the aim of the exam process (what you aim to achieve by the way the process is set)?**
   It is for the process to be secure and to preserve the integrity of the exam papers, and for the process to be belt with quickly and swiftly as possible.
3. **The interest of the research study lies with the setting of examination papers. What does the process of setting examination papers entail?**
   Well the exam papers is set by the examiner, once the examiner is finished, the paper needs to be moderated. The paper can either be internally moderated or externally moderated. If it is internally moderated the examiners needs to ensure that the paper is moderated before the paper is brought to the Examinations Office. However, if the paper is externally moderated it needs to be brought to the Examinations Office and the assigned Examinations Officer then sends the paper to the moderator. Once the paper is back from the moderator, the Examinations Officer informs the examiner and if there are any changes to be made the paper is sent back to the examiner.
4. **What are the challenges that are currently facing the Examinations Office?**
   The hand delivery of exam papers by lecturers who are from the various campuses, poses a problem and the other issue is getting the papers to and from external moderators, the current way is not quiet conducive. If we can get that in a secure electronic way, it will be helpful and effective.
   We also trying to have a look at the system that the UJ is using, we were told about it by a lecturer in the Engineering Department.
   There is also the issue of the paper- base system currently being used, which is a bit challenging to keep a paper trail, which the auditors also raised as an issue and concern.
5. **Is there any other issues raised by the auditors, which are a security concern?**
   The most concern from the auditor's side was the receipting, which is challenging keeping a trail, and currently we are working on an electronic receipting, which will help in keeping a trail on the exam papers.

You can speak to the internal auditor for the exam process, who can share more light on some of the pitfalls of the exam process.

6. **Were there any framework or best practices that you followed when structuring the process and for the development of the examinations policy?**
   We are members of the Examination Administrators Forum. The forum has some best practice guidelines for the examinations process, which we had a look at and because of the merger (that happened between the University of Port Elizabeth, the technikon and the college) we also looked at the different institutions and their processes and tried to incorporate the best qualities and tailor make the current process. We also looked at what other institutions are doing and also used that.
7. **Did you use any person with an information security background to assist, or even follow any information security best practices?**
   NO. To me when we talk about information security, I think electronic, and because we are more paper-based, I didn't think information security is applicable. Currently we use the expertise of the ICT department to help with any technological queries that we have or where there is electronic involvement.
8. **Are there any documented policy and procedures for the process of setting examination papers?**
   There is an examination policy, which addresses the entire examination process. It includes timetabling; exam venues; procedures aimed at students for the exam period; as well as procedures for setting exam papers. There is a lot more regarding exams
9. **How are the documentation communicated to the relevant people?**
   The policy is on the portal and the staff is supposed to know where to find policy. Communiques are also sent out if there are any changes to the policies. We also send out communiques to remind the academic staff of various exam dates, for example, the due date for the exam papers.
10. **How do you ensure that the relevant people follow the policy?**
    By sending out communiques.

*Deputy Director of Examinations also suggested that the Postgraduate Examination Process be looked into, to improve the process. The process entails thick documents being sent to and from the external examiners by courier. Including that in the study would be helpful for the Examinations Office.

Appendix C – Examiners' Questionnaire



Our Web Survey - Examination Paper Preparation Page 1 of 3

Examination Paper Preparation

Page: 1

This questionnaire aims to gain insight on examiners' practices during the preparation of examination papers. The results of this questionnaire will provide feedback for a research study on possible ways of improving the examination process to be more flexible for examiners, yet secure. Participation is completely voluntary. The questionnaires will be anonymous, thus the identity of the participant is not required. The information collected in the questionnaire will be confidential and used for the sole purpose of the research study.

1. Compiling Examination Papers

When setting examination papers

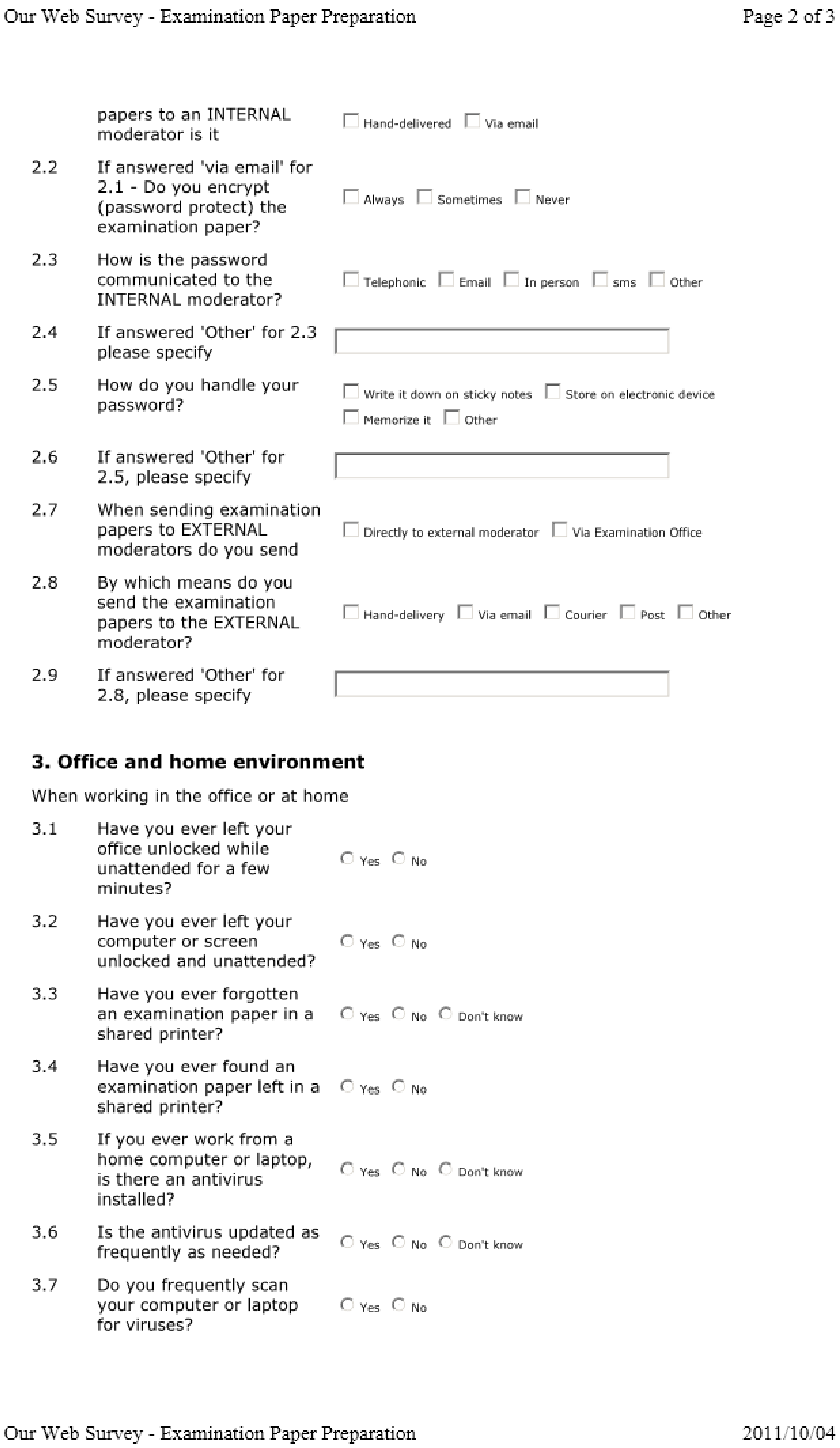
1.1	Do you set examination papers?	○ Yes ○ No
1.2	Where do you prepare your examination papers?	□ Office □ Home □ Both
1.3	Which of the following do you use when setting the examination papers?	□ Computer □ Laptop □ Both
1.4	Which storage devices do you use to save the examination paper?	□ C/drive □ Cloud □ External hard drive □ Flash drive □ Network drive □ Shared drive □ Other
1.5	If answered 'Other' for 1.4 please specify	
1.6	Do you keep a backup copy of the examination paper?	□ Yes □ No □ Sometimes
1.7	Which of the storage devices do you normally use to save the backup copy?	□ C/drive □ Cloud □ External hard drive □ Flash drive □ Network drive □ Shared drive □ Other
1.8	Do you know how to encrypt in Microsft Word (password protect)?	○ Yes ○ No
1.9	When do you discard any draft or spoilt copies of your examination papers?	○ Before the examination ○ After the examination
1.10	How do you discard the examination papers?	○ Throw in dustbin ○ Shred

2. Communicating with moderators

When sending examination papers to moderators

2.1 When sending examination

Our Web Survey - Examination Paper Preparation 2011/10/04



Our Web Survey - Examination Paper Preparation Page 2 of 3

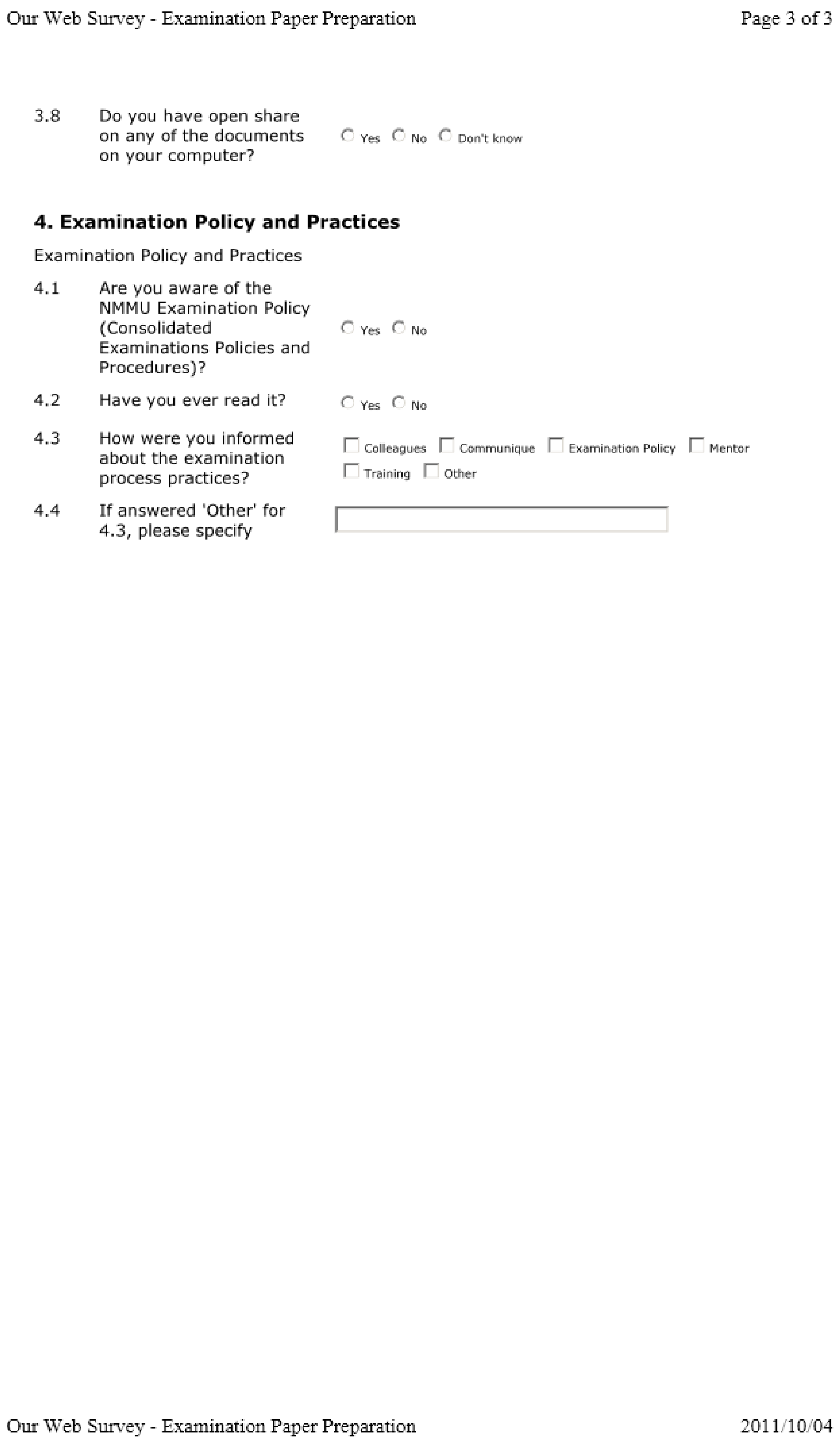
	papers to an INTERNAL moderator is it	□ Hand-delivered □ Via email
2.2	If answered 'via email' for 2.1 - Do you encrypt (password protect) the examination paper?	□ Always □ Sometimes □ Never
2.3	How is the password communicated to the INTERNAL moderator?	□ Telephonic □ Email □ In person □ sms □ Other
2.4	If answered 'Other' for 2.3 please specify	
2.5	How do you handle your password?	□ Write it down on sticky notes □ Store on electronic device □ Memorize it □ Other
2.6	If answered 'Other' for 2.5, please specify	
2.7	When sending examination papers to EXTERNAL moderators do you send	□ Directly to external moderator □ Via Examination Office
2.8	By which means do you send the examination papers to the EXTERNAL moderator?	□ Hand-delivery □ Via email □ Courier □ Post □ Other
2.9	If answered 'Other' for 2.8, please specify	

3. Office and home environment

When working in the office or at home

3.1	Have you ever left your office unlocked while unattended for a few minutes?	○ Yes ○ No
3.2	Have you ever left your computer or screen unlocked and unattended?	○ Yes ○ No
3.3	Have you ever forgotten an examination paper in a shared printer?	○ Yes ○ No ○ Don't know
3.4	Have you ever found an examination paper left in a shared printer?	○ Yes ○ No
3.5	If you ever work from a home computer or laptop, is there an antivirus installed?	○ Yes ○ No ○ Don't know
3.6	Is the antivirus updated as frequently as needed?	○ Yes ○ No ○ Don't know
3.7	Do you frequently scan your computer or laptop for viruses?	○ Yes ○ No

Our Web Survey - Examination Paper Preparation 2011/10/04



Our Web Survey - Examination Paper Preparation Page 3 of 3

3.8 Do you have open share on any of the documents on your computer? ○ Yes ○ No ○ Don't know

4. Examination Policy and Practices

Examination Policy and Practices

4.1 Are you aware of the NMMU Examination Policy (Consolidated Examinations Policies and Procedures)? ○ Yes ○ No

4.2 Have you ever read it? ○ Yes ○ No

4.3 How were you informed about the examination process practices? □ Colleagues □ Communique □ Examination Policy □ Mentor □ Training □ Other

4.4 If answered 'Other' for 4.3, please specify □

Our Web Survey - Examination Paper Preparation 2011/10/04

Appendix D – Threat-source/ Threat-action Tables

Threat-Source/ Threat-Action Tables

Processing State: Confidentiality

THREAT-SOURCE	THREAT-ACTIONS
Hacker	• Remote spying • Gaining unauthorized access to information
Intruder	• Physically gaining unauthorized access to information, by physically gaining unauthorized access to physical environment. • Opportunistically viewing confidential information
Eavesdropper	• Eavesdropping and viewing confidential information
Shoulder surfer	• Observing information without authorization by looking over the shoulder of another or spotting information from a distance.
Employee	• Unauthorized system access • Negligent behaviour and practices
Dumpster diver	• Going through dustbin to retrieve confidential information

Processing State: Integrity

THREAT-SOURCE	THREAT-ACTIONS
Hacker	• Remote spying • Gaining unauthorized access to information for the purpose of modifying
Viruses and worms	• Corrupt files/ documents/ information/ equipment • Alter information
Employee	• Unauthorized system access • Negligent behaviour and practices

Processing State: Availability

THREAT-SOURCE	THREAT-ACTIONS
Hacker	• Opportunistically stealing unprotected information • Denial of service attack
Viruses and worms	• Corrupt files/ documents/ information/ equipment • Denial of service
Thief	• Illegal taking of equipment/ devices / documents
Employee	• Unauthorized system access • Negligent behaviour and practices

Storage State: Confidentiality

THREAT-SOURCE	THREAT-ACTIONS
Hacker	• Remote spying • Gaining unauthorized access to information
Intruder	• Physically gaining unauthorized access to information, by physically gaining unauthorized access to physical environment. • Opportunistically viewing confidential information
Eavesdropper	• Eavesdropping and viewing confidential information
Shoulder surfer	• Observing information without authorization by looking over the shoulder of another or spotting information from a distance.
Thief	• Illegal taking of equipment/ devices / documents
Dumpster diver	• Going through dustbin to retrieve confidential information
Employee	• Unauthorized system access • Negligent behaviour and practices

Storage State: Integrity

THREAT-SOURCE	THREAT-ACTIONS
Hacker	• Remote spying • Gaining unauthorized access to information for the purpose of modifying the information
Viruses and worms	• Corrupt files/ documents/ information/ equipment • Alter information
Employee	• Unauthorized system access • Negligent behaviour and practices

Storage State: Availability

THREAT-SOURCE	THREAT-ACTIONS
Hacker	• Remote spying • Opportunistically stealing unprotected information • Denial of service attack
Viruses and worms	• Corrupt files/ documents/ information/ equipment • Denial of service
Thief	• Illegal taking of equipment/ devices / documents
Employee	• Unauthorized system access • Negligent behaviour and practices

Transmission State: Confidentiality

THREAT-SOURCE	THREAT-ACTIONS
Hacker	• Remote spying • Intercepting unencrypted communication

Intruder	• Physically gaining unauthorized access to information, by physically gaining unauthorized access to physical environment. • Opportunistically viewing confidential information
Eavesdropper	• Eavesdropping and viewing confidential information
Shoulder surfer	• Observing information without authorization by looking over the shoulder of another or spotting information from a distance.
Employee	• Unauthorized system access • Negligent behaviour and practices

Transmission State: Integrity

THREAT-SOURCE	THREAT-ACTIONS
Hacker	• Remote spying • Intercepting unencrypted communication and modifying information
Viruses and worms	• Corrupt files/ documents/ information/ equipment • Alter information
Employee	• Unauthorized system access • Negligent behaviour and practices

Transmission State: Availability

THREAT-SOURCE	THREAT-ACTIONS
Hacker	• Remote spying • Opportunistically stealing unprotected information • Denial of service attack
Viruses and worms	• Corrupt files/ documents/ information/ equipment • Denial of service
Thief	• Illegal taking of equipment/ devices / documents
Employee	• Unauthorized system access • Negligent behaviour and practices

Appendix E – Threat/vulnerability Combination

Threat/Vulnerability Combination

	Confidentiality	Integrity	Availability
		Setting Stage	
Processing	Threats: • Hacker remote spying and gaining unauthorized access to examination papers. • Intruder physically gaining unauthorized access to information, by physically gaining unauthorized access to physical environment and opportunistically viewing confidential information. • Eavesdropper eavesdropping and viewing confidential information • Shoulder surfer observing information without authorization by looking over the shoulder of the another or spotting information from a distance Vulnerabilities: • Leaving office doors unlocked and unattended • Leaving computer screens unlocked and unattended • Not keeping a clean desk policy • Not shredding hard copies of draft examination papers	Threats: • Viruses and worms corrupt files/ documents/ information/ equipment and alter information • Intruder physically gaining unauthorized access to information, by physically gaining unauthorized access to physical environment and opportunistically make changes to confidential information. Vulnerabilities: • Not having anti-virus on computer • Not updating anti-virus • Not frequently scanning for viruses • Leaving office doors unlocked and unattended • Leaving computer screens unlocked and unattended	Threats: • Viruses and worms corrupt files/ documents/ information/ equipment Vulnerabilities • Not having anti-virus on computer • Not updating anti-virus • Not frequently scanning for viruses
Storage	• Not encrypting stored examination papers		• Not keeping a backup copy of the examination paper • Backing up examination papers on the same system or storage device.
Transmission	Not encrypting examination papers emailed to other role players		

Appendix F – Risk List

ITEM NO.	THREAT-SOURCE/VULNERABILITY	IMPACT
IR1	Hacker/unencrypting	Unauthorized access can be gained to unencrypted examination papers while on storage or intercepted email communication.
IR2	Hacker/ineffective password communication	Unauthorized access to passwords can be gained through intercepted email communication or sent messages on lost mobile phones, resulting to unauthorized access to examination papers.
IR3	Hacker/open shares	Unauthorized access to stored examination papers gained through open shares.
IR4	Viruses & worms/no antivirus	Viruses or worms, through infected emails for instance, can corrupt the examination papers, or destroy a storage device, or cause a denial of service. Papers may even be altered due to viruses.
IR5	Viruses & worms/not updating antivirus	Not updating the antivirus software could cause the antivirus to be ineffective in detecting viruses, thereby, causing the corruption of examination papers, or destruction of storage devices, or denial of service, as well as altered papers.
IR6	Viruses & worms/not scanning	Not frequently scanning for viruses can cause undetected viruses or worms to replicate and corrupt examination papers, or destroy storage devices, or cause a denial of service.
IR7	Viruses & worms/no backup	If viruses or worms corrupt examination papers, or the storage device where the paper is stored in, and there is no backup, then the paper may not be available.
IR8	Intruder/unlocked office	Unlocked and unattended offices can give intruders the opportunity to gain access to examination papers, and can even steal equipment and storage devices with examination papers stored in them.
IR9	Intruder/unencrypting	Thief who has stolen equipment or storage devices can gain access to unencrypted examination papers stored in the stolen equipment or devices.
IR10	Intruder/no backup	Stolen examination papers that are not backed up can mean unavailability of examination papers.
IR11	Intruder/unlocked screen	Unlocked and unattended computer screens can give intruders an opportunity to gain access to examination papers.
IR12	Intruder/unlocked door/unlocked screen	Unlocked and unattended computer screens can give intruders an opportunity to make unauthorized changes examination papers.
IR13	Intruder/papers left in printer	Unauthorized access can be gained to examination papers left in printers, especially shared printers. The intruder can make a copy without anyone knowing, or can steal that copy of the examination paper.
IR14	Intruder/not shredding	Intruder can gain access to an examination paper not shredded and in a dustbin.
IR15	Intruder/no clean desk policy	Intruder can opportunistically gain access to unprotected examination paper on the desk. The unprotected examination paper left on a desk can be stolen.
IR16	Eavesdropper/unlocked screen	An eavesdropper can eavesdrop and view an examination paper on screen whilst taking to the examiner.
IR17	Eavesdropper/no clean desk policy	An eavesdropper can view an unprotected examination paper on the desk whilst taking to the examiner or moderator.
IR18	Shoulder surfer/unlocked screen	A shoulder surfer viewing examination papers on screen from a distance or over the shoulder of the unaware examiner
IR19	Shoulder surfer/no clean desk policy	A shoulder surfer viewing from a distance or over the shoulder, an uncovered examination paper on a desk.
IR20	Dumpster diver/no shredding	Dumpster divers can gain access to examination papers thrown in dustbin without being shredded.

Appendix G – Security Controls List

Security Controls List

SECURITY CONTROLS CATALOG	SECURITY CONTROLS	ISO/IEC 27002	NIST SP800 - 53 REV 3
Access Control **(**Control access to information, by ensuring that only authorized persons have access to systems and networks**)**	• Employ access control policies and access enforcement mechanisms to control access between user and object	9.1.1	AC-3
	• Authorized users of information systems should be identified and access privileges specified • Access to system should be granted based on a valid access authorization	9.2.1	AC-2
	• Secure log-on procedures to control access to operating systems in order to minimize opportunity for unauthorized access • Limit number of unsuccessful log-on attempts allowed • Enforce a limit of consecutive invalid login attempts by a user • Automatically deny access when maximum number of unsuccessful attempts is exceeded	9.4.2	AC-7
	• Session lock must be initiated by system after a defined period of inactivity and access should be established using identification and authentication procedures	11.2.8	AC-11
	• Remote access needs to be authorized prior to allowing connection • Unauthorized remote access to system should be monitored	11.4.4	AC-17
User Identification and Authentication **(**Ensures that users are identified and authenticated, before access to systems can be granted**)**	• All users should have a unique identifier (used ID) for their personal use only, and be authenticated by use of mechanisms such as passwords • The information system should uniquely identify and authenticate users	9.2.1	IA-2
	• Systems for managing should ensure quality passwords • Systems should enforce a choice of quality passwords • Systems should enforce users to change temporary passwords at first log-on	9.4.3	
User Responsibilities **(**Ensure cooperation of authorized users to ensure effective security. Users should be made aware of	• Users should be required to follow good security practices in the selection and use of passwords • Passwords should be kept confidential • Strong passwords should be selected • Passwords should be changed regularly, especially when there's a possibility of the password being compromised	9.3.1	

	• Users should ensure that unattended equipment has appropriate protection • Users should be made aware of security requirements and procedures for protecting unattended equipment	11.2.8	
	• A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted. • Computers and terminals should be left logged off or protected with a screen lock when left unattended • Confidential and sensitive documents should be removed from printers immediately	11.2.9	
Mobile Computing and Communications (Ensuring that information is secured when using mobile computing and communications facilities)	• A formal policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communications facilities (e.g. notebooks, laptops, mobile phones, ipads) • Special care should be taken to ensure that business information is not compromised. • Policy should include the requirements for physical protection, access control, cryptographic techniques, backup and virus protection • Protection should be in place to avoid unauthorized access to, or disclosure of the information stored, processed or transmitted by these facilities (e.g. use of cryptographic techniques) • Procedures against malicious software should be in place and be kept up-to-date • Mobile computing facilities should also be physically protected against theft.	6.2.1	SI-3
Cryptographic Controls To protect the confidentiality and integrity of information by cryptographic means	• Policy on the use of cryptographic controls should be developed and implemented • The use of encryption for protection of sensitive information transported by mobile, or media devices, or across communication lines.	10.1.1	
Information Security Policy To provide management direction and support	• Information security policy document should be published and communicated to all employees • Review of information security policy should be performed at planned intervals or if significant changes occur to ensure its continuing suitability	5.1.1 5.1.2	
Internal organization To manage and control information security within the organization	• Information security responsibilities should be clearly defined; responsibilities for the protection of information assets and for carrying out specific security processes should be clearly identified. • Contact with special interest groups should be maintained; to improve knowledge about best practices and staying up to date with relevant security information • Independent review of information security should be performed; to assess opportunities for improvement and the need to change policy and controls.	6.1.1 6.1.4 6.1.5	AT-5

Responsibility for assets To achieve and maintain appropriate protection of organization assets.	- Acceptable use of assets; rules for acceptable use of information and assets associated with information processing facilities should be identified, documented and implemented. - Guidelines for the use of mobile devices	8.1.3	MP-4
Secure area To prevent unauthorized physical access, damage and interference to organization premises and information	- Securing offices, rooms and facilities; physical security for office should be designed and applied.	11.1.3	PE-2
Protection against malicious code To protect the integrity of software and information	- Controls against malicious code; detection, prevention and recovery controls to protect against malicious code and appropriate user awareness procedures should be implemented. - Installing and regular update of malicious code detection and repair software to scan computers and media as a precautionary control	12.2.1	SI-3
Back-up To maintain the integrity and availability of information and information processing facilities	- Adequate back-up facilities should be provided to ensure all essential information and software can be recovered following a disaster or media failure.	12.3.1	CP-9
Media handling Appropriate operating procedures to protect document and computer media or disks	- Procedures for handling and storage of information should be established to protect information from unauthorized disclosure or misuse. (Procedures for handling, processing, storing and communicating information) - Access restrictions to prevent access from unauthorized persons	8.3.3 8.3.1	MP-4 MP-5

Exchange of information To maintain the security of information and software exchanged within the organization and with any external	• Information exchange policies and procedures; should be in place to protect the exchange of information through the use of all types of communication facilities. • Procedures and controls when using electronic communication facilities for information exchange; procedure designed to protect from interception, copying, modification, destruction. • Not leaving sensitive information on printing facilities e.g. copiers, printers as these may be accessed by unauthorized persons • Physical media in transit; media containing information should be protected against unauthorized access, misuse, or corruption during transportation beyond organizations physical boundaries. • Electronic messaging; information involved in electronic messaging should be appropriately protected (Electronic messaging, such as email play an increasingly important role in business communities. It has different risks than paper based communications)	13.2.1 13.2.3	AC-21 PE-5 MP-5
Monitoring Systems should be monitored and information security events should be recorded	• Audit logging • Monitoring system use (to keep records and monitor unauthorized activities)	12.4.1 12.7.1	AU-3
Compliance with information security policies To ensure compliance of systems with organizational security policies	• Managers should ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.	18.2.2	
Training awareness education	• Management should initiate plans and programs for maintaining information security awareness • Management should effectively promote information security awareness, education and training throughout the organization • Information security awareness, education and training requirements should be documented in the policy • Adequate level of awareness, education and training in security procedures and correct use of information processing facilities should be provided to minimize possible security risks • Users should receive appropriate awareness training and regular updates in organization policies and procedures relevant for their job functions	7.2.2	AT-2 AT-1 AT-4

Appendix H – ISAM Detailed Guide

PHASE: ESTABLISH PLAN

Description:

This phase concerns planning what needs to be in place and identifying events that could affect the aim of what needs to be in place. The phase involves the planning and assessing of a certain process to determine if the process meets its set objectives. During this phase information security concerns need to be taken in to consideration, in order to ensure that the process concerned is secure and preserves the confidentiality, integrity and availability of its information assets. Therefore risks pertaining to the process need to be assessed and appropriate actions identified in order to mitigate those risks. A policy also needs to be established during this phase, in order to give direction and guide actions. The current state of the process needs to be known in order to decide if further actions need to be taken to ensure that the process is the way it is meant to be.

During this phase decisions on which process to look at should be made; the identification of the process to be assessed. The scope and boundary of what is to be assessed should be determined, as well as the objectives clearly defined. The phase should also include the purpose of the process, as well as the aim of the process (what is to be achieved by the process).The phase should take into account the security of the information assets within the identified process.

The Output of the Phase:

Objectives of the process or system being assessed.
Risk assessment report; detailing the identified risks pertaining to the process or system.
Policy (which reflects the security of information assets, such as examination papers)
List of relevant security controls

Guiding Questions:

1. Which process is being looked at?
(E.g. The examination paper preparation process)
2. What is the scope and boundary of the process?
(E.g. The process will include the setting, the moderation, the authorizing of the examination papers and end with the submission of the examination paper at the examinations office. The process will include only the internal moderators)
3. Which ICT resources used in the process will be included; that needs to be addressed?
(E.g. The various processing, storage and transmission technologies used by examiners and moderators during the process of preparing examination papers)
4. What is the aim of this assessment effort?
(E.g. To improve the security of the examination papers during the process of the papers being prepared; by ensuring that all relevant aspects are considered and addressed)
5. What are the threats that pertain to the environment that is being assessed?
6. What are the vulnerabilities that exists or could exist; that could be exploited by the identified threats, thereby causing risk to the security of the examination papers and the process as a whole?
7. What existing security controls are in place, for guarding against the threats?

Suggestions:

1. Any exclusion in the scope and boundary must be documented with reason for the exclusion.
(E.g. External moderation will be excluded. This will be addressed separately as part the process from the examinations office side)
2. Involve the ICT service department. This joint effort will assist in identifying all the threats; including those to the networks and information systems that might be used during the process.
(E.g. Students using tools to sweep the networks for open sources/shares in order to gain access to lectures drives. Therefore, ICT services will help in communicating this, making examiners and moderators aware, and provide assistance in ensuring that shares are closed or opened to all those with authorization)

Action Plan:

Actions to be taken are:
EP1 - Establish context
EP2 - Perform analysis of existing policies and security efforts
EP3 - Perform risk assessment
EP4 - Establish policy
EP5 - Identify relevant security controls

WHAT:	**EP1 - ESTABLISH CONTEXT**
WHY:	To get all the necessary information required to start any project. To know which process is being dealt with, the structure of the process, as well as what the process entails. To identify the objectives and aim of the process. Further, to identify the role players in the identified process, as well as the ICT resources used within the process.
HOW:	• By identifying the **process** to be assessed and determining the structure of that process, in order to understand the workflow and what the process entails. • By identifying the **information assets** in the process, which require protection. • By defining the process' **scope and boundary**. Defining the scope and boundary will help ensure that all relevant information assets are taken into account in the assessment, as well as identifying the ICT resources used for the processing, storage and transmission of the information assets. • By including the **purpose** and **aim** of the identified; this will help in giving direction as to what needs to be achieved. • By clearly defining the **objectives** of the process. Objectives help define what needs to be achieved. The objectives need to take in to consideration the mission and vision of the institution, so as to ensure that the identified process supports the mission and vision.
WHO:	The management team responsible for setting up the identified process is responsible for establishing the context. The individuals involved in the process can help in the identification of the various ICT resources they use for the processing, storage and transmission of the information assets.
WHAT:	**EP2 - PERFORMING ANALYSIS OF EXISTING POLICIES AND DETERMINE CURRENT SECURITY EFFORTS**
WHY:	To determine what policies and procedure are currently in place. Further to ascertain if the current policies and procedures, as well as the security posture of the identified process reflects the defined objectives, and to what extent are the objectives addressed by the current policy and security posture. The information will assist in determining the need for any adjustments, as well as determining the way forward, and understanding the amount of work that needs to be done, in order to achieve the objectives as set in EP1.

HOW:	• By basing it on the **aim** and **objectives** identified in EP1. • By performing an analysis of the policies, procedures and security efforts pertaining to the identified process. • By determining whether what is in place meets the aim and the identified objectives of the process, or whether something needs to be done in order to address the **shortfall** (identifying the gap).
WHO:	The management team responsible for setting up the identified process is the responsible party for determining what is currently in place, and what needs to be in place (the process owner).
WHAT:	**EP3 - PERFORM RISK ASSESSMENT**
WHY:	Before you can address the **shortfall (EP2)**, and in order to meet the **objectives (EP1)** of the process, an **assessment of risks** need to be performed. The risk assessment will assist in identifying anything that will prevent the objectives to be met. Risk assessment will also help in determining and understanding the implications of the risks to the process and the institution as a whole.
HOW:	Risks to the process need to be identified, in order to determine the security needs of the process, so that appropriate and adequate security controls can be selected to mitigate those risks. When identifying risks, ensure that you consider the practices of the role players, which could compromise the information assets, in order to address those. Also consider which ICT resources are used by the role players for the processing, storage and transmission of the information assets. The following needs to be done, in order to Identify the risk: • Identify the information asset (what is to be protected). • Identify the various ICT resources used to process, store and transmit the information assets (such as personal computers, laptops, flash drives, and the Internet). • Identify the potential threats associated with the process. Threats are any potential cause of unwanted incidents that could compromise the security of the information assets. Remember to consider the threats associated with the use of the ICT resources as well. • Identify potential vulnerabilities pertaining to the identified process. Vulnerabilities are any weaknesses, which could be exploited by threats, thereby compromise the security of the information assets. The role players practices should also be considered, those practices that could be vulnerabilities which could be exploited, thereby compromising the security of the information assets (e.g. leaving doors and computers unlocked and unattended, not encrypting electronically stored or transited information assets) • Determine the impact to the process and/or institution, should the threat exploit the vulnerability, compromising the security of the information assets (e.g. bad publicity thereby damaging institution's reputation, leading to decrease in registering students and donations, resulting in financial loss to the institution). • Determine the risks to the process, in order to determine the information security requirements that will need to be satisfied, for the information assets to be sufficiently protected. When identifying risks, certain practices and behavior of role players that might compromise the security of the information assets need to be considered, in order to appropriately address it. The **Risk List** can be used as guidance for identifying the risks to the process.
WHO:	The management team (and/or process owner) responsible for setting up the identified process is responsible for determining what the risk to the process are and how appropriate to deal with those risks. The management team can sought out help from various departments and professionals, such as the Risk Management and Auditing Departments. ICT Services Department also needs to be involved, in order to identify threats and vulnerabilities associated with ICT systems and networks. The individuals involved in the process can also assist, as they are the individuals who understand the process and work with it almost daily, so they can shed a light in to their practices, so that inappropriate practices that could be vulnerabilities could be identified and addressed.

WHAT:	**EP4 - ESTABLISH POLICY**
WHY:	Once the risks have been identified, and the information security needs been determined, a policy (that reflects the secure preparation of examination papers) needs to be established. The policy needs to take in to consideration the information assets that require protection and any information security concerns, in order to ensure a secure process. The policy should be based on information security best practices for developing an information security policy (ref. to the **HOW**). . The policy is a direction-giving document, which provides management with direction and support ensuring a secure process. It is written to support the aim and objectives of the identified process, and specifies and dictates acceptable and unacceptable behaviour for all role players involved in the process. It provides a set of rules for the protection of information assets within the process, and directs how issues should be addressed. It further defines and documents the appropriate processes and procedures needed to counter the risks identified in the risk assessment, in order to secure the process. The policy, therefore, becomes the baseline for the appropriate action to be taken, and the security controls to be selected and implemented.
HOW:	For the policy to be effective, it requires the following: • State management commitment to preserving the confidentiality, integrity and availability of the information assets. • Express the security needs of the process, by addressing the information security requirements identified in the risk assessment. • Define the roles and responsibilities of all role players regarding secure handling of information assets (secure processing, storage and transmission). • Inform role players of acceptable and unacceptable behaviour while handling the information assets. • Make role players aware of certain security issues and provide means of dealing with those issues. • The policy should be considered a living-document that requires constant modification and maintenance as changes develop and the needs of the process evolve. • Should be reviewed at least annually. • The policy needs to be properly communicated and made available by all means possible to all relevant people. The policy also needs to be read, understood and agreed to by all relevant people. • The policy should be clear and precise, with no room for misinterpretations. • Consequences of policy violations must be clearly stated.
WHO:	The management team (and/or process owner) responsible for setting up the identified process, is the responsible party for establishing the policy, and ensuring that all relevant people are aware of the policy and that the policy is disseminated to them. Role players involved in the identified process should ensure that they read and understand the policy.
WHAT:	**EP5 - SELECTION OF RELEVANT SECURITY CONTROLS**

WHY:	Once the risks have been identified, the information security needs determined and the policy established; relevant security controls can be identified and selected. The **Security Controls List** can be utilized as guidance for the selection of appropriate controls for the identified risks (**EP4**). Appropriate actions and relevant security controls are identifies and selected, in order to satisfy the information security requirements identified in the risk assessment, in order to provide the needed level of protection for the information assets and in creating a secure process. Security controls are specific security-related activities and/or actions carried out to protect information assets. These are the safeguard measures employed to counter risk and protect the confidentiality, integrity and availability of the information assets.
HOW:	The right mix of controls from the three categories needs to be selected in order to provide adequate and effective protection for the information assets, and for the creation of a secure process. The management controls, which are the management actions, entails: planning what needs to be in place, ensuring that risk assessment is performed, policy established, and roles and responsibilities defined. Operational controls entails: awareness, training and education programs for all role players, ensuring that physical and environmental security is in place, and personnel security dealt with (personnel reliable and trust worthy). Technical controls are the technology controls: hardware and software controls, which deal with access control to information systems and networks, identification and authentication, audit and accountability, and information systems and communication protection.
WHO:	The management team responsible for setting up the identified process is responsible for identifying and designing the required security controls. The management team can sort out assistance from the ICT Service Department for the selection of the technical controls.

PHASE: IMPLEMENT & OPERATE

Description:

This phase deals with ensuring that the policy is implemented, as well as ensuring that the identified and selected security controls from the Establish Plan phase are implemented and operating properly.

In this phase an awareness, education and training program needs to be in place, in order to ensure that all role players are aware of their roles and responsibilities towards the protection of the information assets. Further, the program will ensure that the role players are aware of the risks pertaining to the identified process and that they are equipped in dealing with those risks. The program will further ensure that the policy is distributed to all relevant people and that the people read and understand the policy.

At this phase, there should also be a plan to ensure that the implemented policy and security controls are reviewed, to ensure that they are effective in their intended operation.

The Output of the Phase:

Documentation of all implemented management, operational, and technical controls, relevant for the identified process.
Documented awareness, education and training program, and the timeline for the implementation of the program
A review plan for the effectiveness of the implemented security controls and awareness, education and training program

Guiding Questions:

1. Are the selected security controls relevant and adequate for the protection of the information assets?
2. Has the ICT Service Department been sufficiently involved and has it communicated what we need to know?
3. Are we aware of and understand how the various technical controls operate.
4. How will the ICT Service Department be involved in the awareness, education, and training program?
5. What other relevant professionals can we approach to assist with the policy and the Awareness, education and training program?
6. Have all the security controls been implemented and are they operating effectively?
7. Have the role players been made aware of the associated risks and the various controls that are in place, and do they know how to operate the controls?

Suggestions:

1. Try to ensure that procedures are not too technology specific because technology changes overtime. E.g. Providing an encryption procedure based on Office 2007 could be different for individuals using Office 2010.

Action Plan:

Actions to be undertaken are:
1. Implement policy
2. Implement security controls
3. Develop and implement an awareness, education and training program
4. Develop a plan for monitoring and reviewing of risks, policy and security controls

WHAT:	**IO1 - IMPLEMENT POLICY**
WHY:	Implementing the policy serves as a template for the implementation of the rest of the security controls.
HOW:	Ensure that for each policy statement there is a security control selected and implemented The policy statements can be implemented as either processes, procedures or technical controls Ensure that the policy meets the security requirements identified by the risk assessment.
WHO:	The management team responsible for setting up the identified process is responsible for ensuring that the policy is implemented and that the role players are aware of the policy and what is expected of them in terms of the policy. The individuals involved in the process are responsible for following what is set in the policy.
WHAT:	**IO2 - IMPLEMENT SECURITY CONTROLS**
WHY:	The selected security controls need to be implemented in order to mitigate the identified risks. The security controls need to be assessed to ensure that they operate as intended.
HOW	Ensure that the selected security controls are implemented. Ensure that ICT services have implemented the identified technical controls. Ensure that role players are aware of the procedures they need to follow. Ensure that is role players using personal ICT resources for processing, storing and transmitting the information assets, they are aware of the controls they need to implement.
WHO:	The management team responsible for setting up the identified process is responsible for ensuring that all selected security controls are implemented and operating as intended. The management team is also responsible for ensuring that the ICT Service department implement the selected technical controls. The individuals involved in the process are responsible for ensuring that security controls are implemented on any personal ICT resources they use for the processing, storage and transmission of the information assets.

WHAT:	**IO3 - DEVELOP AND IMPLEMENT AWARENESS, EDUCATION AND TRAINING PROGRAM**
WHY:	Awareness, education and training program is vital in any information security effort. The program will ensure that role players are aware of and understand the risks pertaining to the process, that they are aware of the nature of the security controls in place for the mitigation of those risks. The program is also meant to assist in ensuring that the role players are educated and trained in what they need to know and do. The program is meant to inform role players of their responsibilities and what is expected of them, as documented in the policy and procedures; it is also meant to explain proper behaviour. The program should assist in changing behaviour and reinforcing good security practices.
HOW:	The program can include: • Presentations and workshops for the role players. • E-learning and internet communication (communiqué). • Training workshops on how to properly use any technical control. • Proper and appropriate communication of policy and procedures that need to be followed.
WHO:	The management team responsible for setting up the identified process is responsible for ensuring that there is an awareness, education and training program in place. The management team is also responsible for ensuring that the ICT Service department is involved and that the department can assist with anything technical and with anything that has to do with networks and ICT systems. The management team should seek advice and assistance from relevant professionals who would assist with setting up awareness, education and training programs and materials. The individuals involved in the process are responsible for ensuring that they sign up for the presentations and training workshops.
WHAT:	**IO4 - DEVELOP A PLAN FOR MONITORING RISKS AND COMPLIANCE, AND REVIEWING POLICY AND SECURITY CONTROLS**
WHY:	Risks need to be constantly monitored to ensure that any new threats and vulnerabilities are addressed. Compliance also needs to be monitored to ensure that policy and security controls are being adhered to. Whenever there are any significant changed to the process or new risks develop; the policy and security controls need to be reviewed. Therefore, there needs to be a plan in place to ensure that the monitoring and review takes place.
HOW:	The plan needs to define how and when to monitor and review; state the individuals responsible for the monitoring and reviewing, and how to deal with the results of the monitoring and reviewing.
WHO:	The management team responsible for setting up the identified process is responsible for developing the plan.

PHASE: MONITOR & REVIEW

Description:

Risks and compliance should be monitored, and policy and security controls reviewed regularly to make certain that these continue to reflect the needs of the process. Any changes should be determined in order for appropriate decisions to be made. This phase deals with ensuring that the risks and compliance are monitored, and the policy and security controls reviewed in order to determine if they are effective in their operations.

Monitoring and reviewing will ensure that the policy and security controls are modified to respond to any events that may impact on the security of the process in question.

The Output of the Phase:

Documented results of the monitoring and review.
Documentation of the decisions made based on the results of the monitoring and review.

Guiding Questions:

1. How do we monitor the risks and compliance?
2. How do we review the policy and security controls?
3. What tools are available which we can use?

Suggestions:

1. Involve the ICT Service Department to ensure that the risks to ICT systems and networks are monitored and technical controls reviewed.

Action Plan:

Actions to be undertaken are:

1. Monitor risks
2. Monitor compliance
3. Review process performance against policy and objectives
4. Review performance of security controls

WHAT:	**MR1 - MONITOR RISKS**
WHY:	Risks to the process need to be monitored regularly to ensure that there are now new risks to the process caused by emerging threats and vulnerabilities.

HOW:	Monitor threats and vulnerabilities, in order to identify new ones. For any changes in the process, ensure that the risk assessment reflects those changes in order to accommodate those changes and account for risks that could exist due to the changes. Ensure that the ICT Service Department have tools and programs to monitor risks to the ICT systems and networks pertaining to the process, and ensure that they communicate any changes, in order to update the policy and security controls.
WHO:	The management team responsible for setting up the identified process is responsible for ensuring that risks are monitored on a regular basis. The management team is also responsible for ensuring that the ICT Service department is involved and that the department monitor risks to the ICT system and networks and that the department communicate the results. The individuals involved in the process are also responsible for monitoring the risks, and that they communicate any events that may impact the security of the process, to the management team.
WHAT:	**MR2 - MONITOR COMPLIANCE**
WHY:	Monitoring compliance is to ensure that any security activities are executed in accordance with the policy. To ensure that individuals comply to the policy. To ensure that individuals adhere to the operations of the security controls
HOW:	Need involve ICT to do regular checks on system, e.g. checking for open shares on the systems. Need to ensure that the policy is properly communicated to role players (they will have to indicate that they have read and understood the policy) Heads of Departments could also check to see if offices are not left unlocked and unattended.
WHO:	The management team responsible for setting up the identified process is responsible for ensuring that compliance is monitored. The ICT Service department is responsible for ensuring that technical security controls are in compliance with the policy, as well as monitoring any online activities that contradict the policy, amongst other things.
WHAT:	**MR3 - REVIEW PROCESS PERFORMANCE AGAINST POLICY AND OBJECTIVES**

WHY:	This is to check if there are any changes to the process, and that those changes are reflected in the policy and that the objectives of the process have not changed. Its to ensure the continuing suitability of the process' security.
HOW:	Check if there are any changes to the scope and boundary of the process. Check if the changes affect the objectives and the policy. Check if the process performance reflects the aim of the policy and objectives (this includes checking everything that is implemented to ensure that the security of the process is improved).
WHO:	The management team responsible for setting up the identified process is responsible for reviewing the process performance.
WHAT:	**MR4 - REVIEW PERFORMANCE OF SECURITY CONTROLS**
WHY:	Implemented security controls need to be regularly reviewed in order to assess their suitability in protecting the information assets. Security controls need to be reviewed to ensure that they operate as intended.
HOW:	Need to know and understand what the particular control is supposed do and how it supposed to perform, and then assess to see if it is performing as intended. Need to have a measurement to measure against. Need to report on the review results in order to take appropriate actions to improve the effectiveness of the security controls.
WHO:	The management team responsible for setting up the identified process is responsible for reviewing the effectiveness of the security controls, and that they ensure that the ICT Service Department review the technical controls. The ICT Service Department is responsible for reviewing the effectiveness of the technical controls and ensuring that they report back to the management team of the identified process.

PHASE: MAINTAIN & IMPROVE

Description:

This phase is for ensuring that the necessary actions are taken based on the results of the Monitor & Review phase.

The Output of the Phase:

Modification of policy and security controls to respond to the findings of the Monitor & Review phase.
Improvement of the effectiveness of the policy and security controls.

Guiding Questions:

1. Are there gaps, control failures or recommendations that we need to relook or implement?

Suggestions:

1. Not all recommendations or suggestions need to be implemented, however, you should document the reasons why you are not going to implement them.

Action Plan:

Actions to be undertaken are:
1. Take appropriate actions based on the results of the Monitor & Review Plan phase.

WHAT:	**MI1 - TAKE APPROPRIATE ACTIONS BASED ON THE RESULTS OF THE MONITOR & REVIEW PLAN PHASE**
WHY:	Appropriate actions need to be taken based on the results, findings and recommendations of the Monitor & Review phase in order to ensure that the information assets are adequately and suitably protected, as well to improve the security of the process.
HOW:	First need to decide whether or not to implement the suggestions and recommendations, if not implementing, then you should document the reasons why. Decide by when the improvements need to be done. Implement the suggestion and recommendations as recommended.
WHO:	The management team (and/or process owner) responsible for setting up the identified process is responsible for ensuring that the appropriate actions are taken, and for ensuring that the ICT Service Department implement any changes that need to be implemented.

Appendix I – Elites' Feedback Form: Examinations

Reviewer Feedback

The purpose of the reviewer questions below is to assist in the evaluation of the ISAM for the Examination Paper Preparation Process (EPPP); by obtaining your opinions and recommendations as reviewers, based on your work experience and knowledge.

Please complete the questions below. Please include comments if you have any.

Reviewer Questions

Demographics			
Please provide the following			
1. Job Title:			
2. Job Description:			
3. No. of years in current position:			
Utility of ISAM			
Please rate each statement: 1 = disagree; 2 = not sure; 3 = agree. Please provide comments if you have any.			
4. From a high-level view of the ISAM; the ISAM is understandable Comment:____ ____ ____ ____	1	2	3

5. The ISAM is relevant for the EPPP Comment:____ ____ ____ _______________________________________	1	2	3
6. The ISAM is adaptable and can be utilized for other processes within the examination process Comment:____ ____ ____	1	2	3
7. The ISAM Detailed Guide provides a clear description of what needs to be accomplished at each phase of the ISAM Comment:____ ____ ____ _______________________________________	1	2	3
8. The ISAM Detailed Guide provides enough information and guidance for the implementation of the ISAM Comment:____ ____ ____ _______________________________________	1	2	3
9. The ISAM will assist in developing an adequate policy for the EPPP Comment:____ ____	1	2	3

______________________________ ________________________			
10. Any other comments, suggestions and/or recommendations __________________________________ __________________________________ __________________________________ ____________________________			

Thank you for taking the time to evaluate the model.

Once completed please email to: miemie.mogale@gmail.com

Appendix J – Elites' Feedback Form: Information Security

Reviewer Feedback

The purpose of the reviewer questions below is to assist in the evaluation of the ISAM for the Examination Paper Preparation Process (EPPP); by obtaining your opinions and recommendations as reviewers, based on your work experience and knowledge.

Please complete the questions below. Please include comments if you have any.

Reviewer Questions

Demographics			
Please provide the following			
11. Job Title:			
12. Job Description:			
13. No. of years in current position:			
Utility of ISAM			
Please rate each statement: 1 = disagree; 2 = not sure; 3 = agree. Please provide comments if you have any.			
14. From a high-level view of the ISAM; the ISAM is understandable Comment:____ ____ ____ ______________________________________	1	2	3

15. From a high-level view the ISAM is relevant for the EPPP Comment:________________________________ ________________________________ ________________________________ __________________________	1	2	3
16. The ISAM comprehensively identifies crucial components that contribute to a secure EPPP Comment:________________________________ ________________________________ ____________________________	1	2	3
17. The ISAM can assist in defining and documenting a secure EPPP Comment:________________________________ ________________________________ ________________________________ __________________________	1	2	3
18. The ISAM can assist in the development of a policy specific for the EPPP, which clearly addresses the security of the examination papers Comment:________________________________ ________________________________ ________________________________ __________________________	1	2	3
19. The ISAM can assist in creating and raising awareness of any security related issues pertaining to the EPPP, for all stakeholders (examiners and examinations officials) Comment:________________________________ ________________________________ ________________________________	1	2	3

20. Any other comments, suggestions and/or recommendations

Thank you for taking the time to evaluate the model.

Once completed please email to: miemie.mogale@gmail.com