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*— This paper has critically assessed a Higher Education Institution's (HEI) Examination Paper Preparation Process (EPPP) to identify threats and vulnerabilities that could place the security of the process at a risk; thus, compromising the security of the examination papers. Surveys were utilized to identify examiners' behaviour which could pose a 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 covered to ensure that examination papers are handled more securely. The aim of the model is to ensure that examination papers are not accessible to unauthorized individuals; which, may lead to some students being conferred with qualifications that they do not deserve.**

***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 [*1*]. 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 that 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 a means of managing and improving the security of a process. Section IV follows with the research methodology. Section V discusses the research results, followed by Section VI, the Information Security Assurance Model (ISAM) and Section VII, the ISAM Components and Guides. 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

978-1-4799-3383-9/14/$31.00 ©2014 IEEE

social, central and economic development of the nation [2]. One of its goals being to ensure national growth and competitive edge; which is dependent on continuous technology improvement and innovation [3]. 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 [4]. 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 [5]. This can be partly 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 [6]. For future employers they give assurance that the passing students have the basic understanding of the work and that they are competent.

However, 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 credibility of 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 which may otherwise 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 until the examinations are written). The process of an EPPP of a particular HEI is depicted in Figure 1.

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, during the four stages that the papers go through, namely 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, 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 may be 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 a means to assist in ensuring an effectively controlled and managed EPPP, which manages and improves the security of the examination papers.

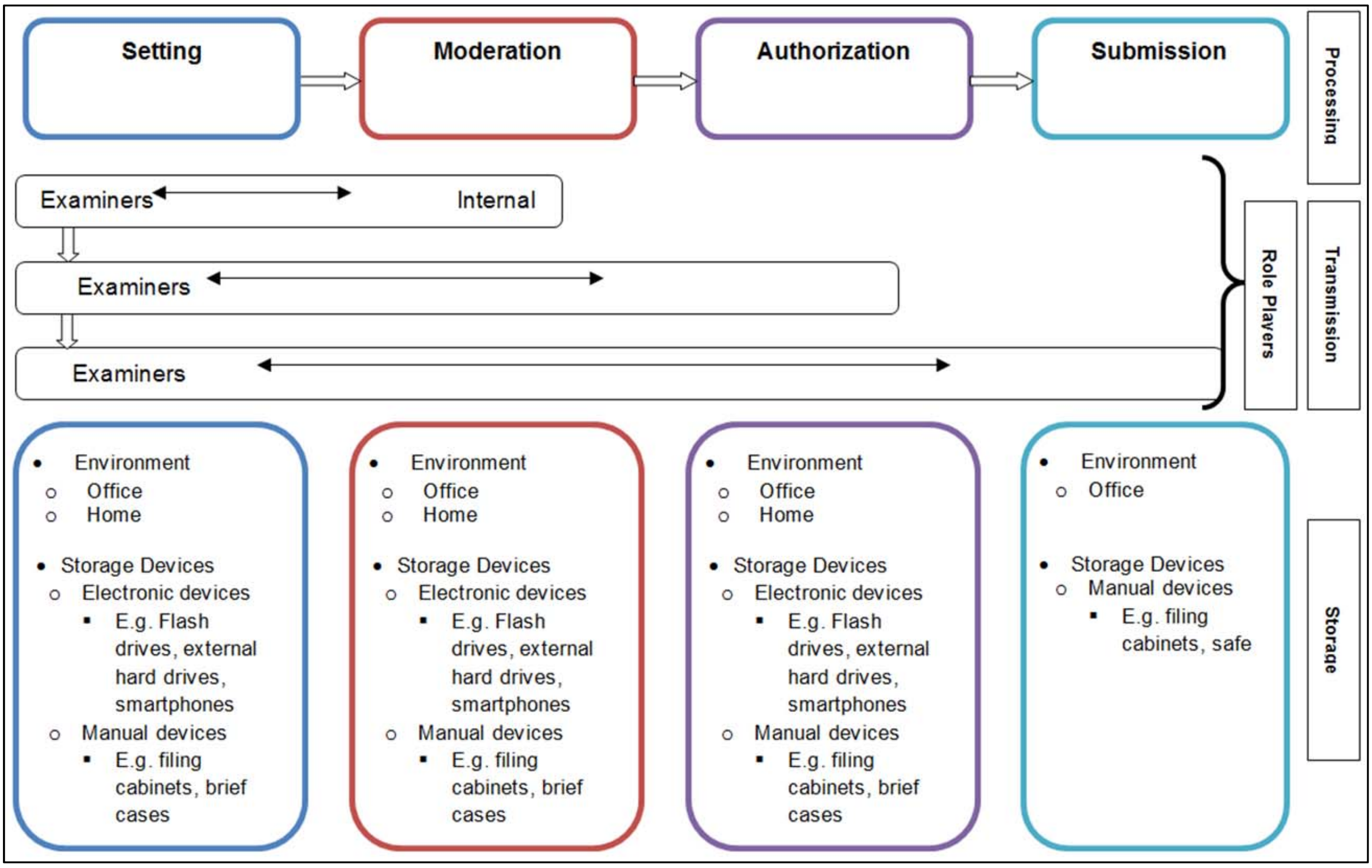


Fig 1. Examination Paper Preparation Process

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 [*7*]. 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 [*8*].

When dealing with the risks, many researchers suggest managing the risks through the implementation of a proper and comprehensive information security management system (ISMS) [*9*] [*10*]. 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 [*11*]. 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' [*12*]. Eloff and Eloff [*9*], 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 [*13*], 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 [*13*] [*14*] [*15*]. A brief discussion on these aspects follows:

- Organizational structure deals with "the way information security is organized and structured in an organization" [*13*]. 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 [*16*] [*17*]. 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" [*18*]. 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 [*13*].
- 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 [*19*] [*20*].
- 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 [*19*] [*17*].
- 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 [*19*] [*13*] [*21*]. 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 [*22*].

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 [*23*], 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 [*23*]. 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 [*23*], 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: if they had left office doors and computer 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 examination 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 examinations 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 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 a few.

From the observation, the author observed that from the Examinations Office side, papers were handled securely. Entrance to the office is limited to 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 without 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 explicitly 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; a 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.

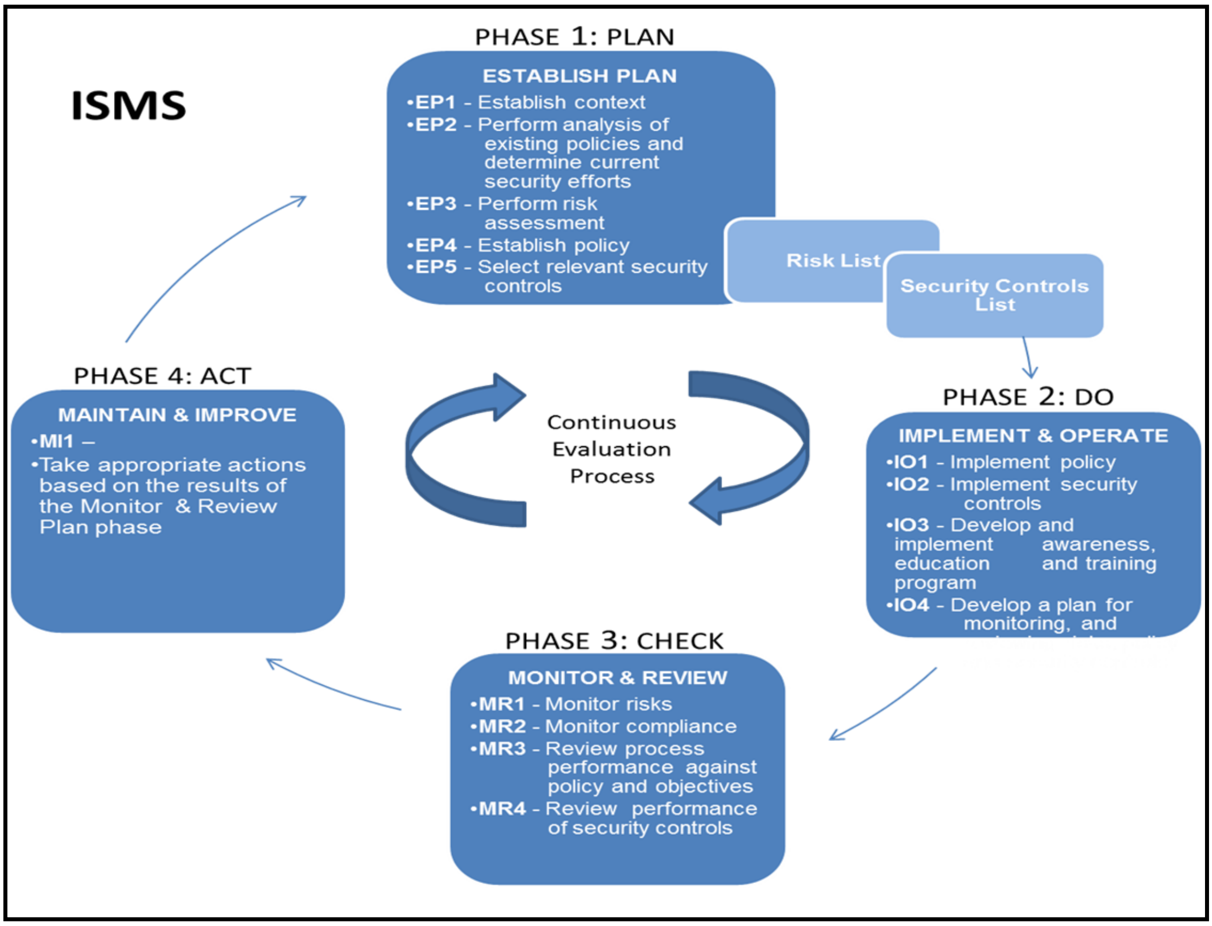

ISMS
PHASE 1: PLAN
ESTABLISH PLAN
•EP1 - Establish context
•EP2 - Perform analysis of existing policies and determine current security efforts
•EP3 - Perform risk assessment
•EP4 - Establish policy
•EP5 - Select relevant security controls
Risk List
Security Controls List
PHASE 2: DO
IMPLEMENT & OPERATE
•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 [*19*] 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.

A. 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.

B. 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.

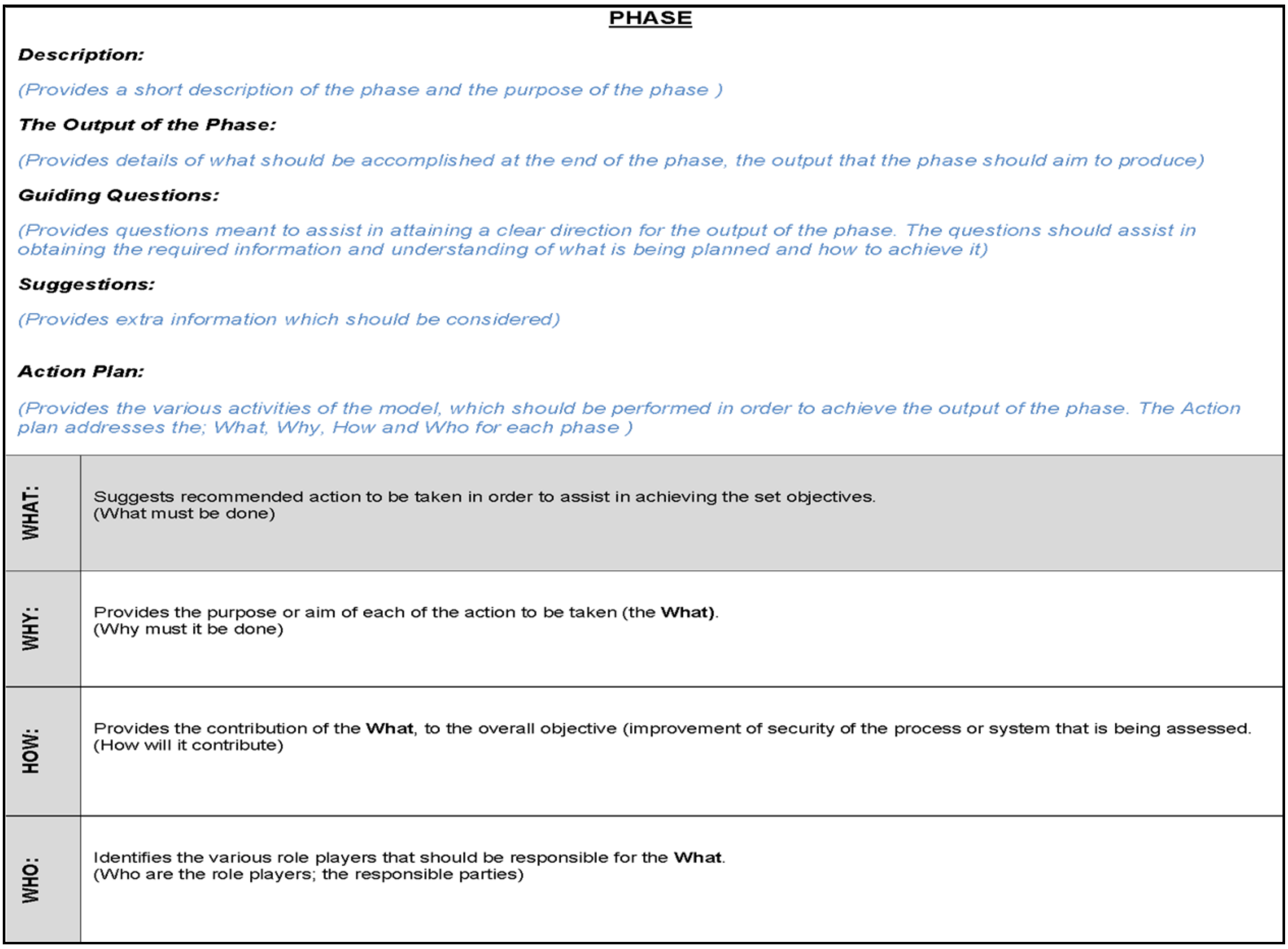
The Security Controls List presents a list of security controls, identified from the ISO 27002 [*19*] and NIST SP-53 Rev 3 [*17*]standards, for the mitigation of the identified risks presented in Table 1's Risk List. The numbering contained in the last two columns of Table III (ISO27002 and NIST SP-53 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 3
Access Control (Control access to information, by ensuring that only authorized persons have access to systems and networks)	11.1.1	AC-3
	11.2	AC-2
	11.5.1	AC-7
	11.5.5	AC-11
	11.4.4	AC-17

C. 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)

Fig 3: ISAM Detailed Guide Template

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

a) *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.

b) *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.

c) *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.

d) *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 HEIs 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 an EPPP policy to ensure that relevant information security aspects are covered to contribute to more secure handling of examination papers.

REFERENCES

[1] J Todd. (2007, July) Helium. [Online]. HYPERLINK "http://www.helium.com/items/436615-what-is-the-impact-of-new-technology-in-the-workplace" http://www.helium.com/items/436615-what-is-the-impact-of-new-technology-in-the-workplace

[2] Minister of Education, A programme for the transformation of higher education, July 24, 1997.

[3] CHE. (2003, June) The council on higher education. [Online]. HYPERLINK "http://www.che.ac.za/sites/default/files/publications/CHE_HE_Monitor_no1_June2003_0.pdf" http://www.che.ac.za/sites/default/files/publications/CHE_HE_Monitor_no1_June2003_0.pdf

[4] SASCO, "Debating institutional autonomy and academic freedom: Search for perspective," in *SASCO 2009 16th National Congress*, 2009.

[5] Minister of Education, National plan for higher education, 2001.

[6] NMMU. (2011, July) Nelson Mandela Metropolitan University. [Online]. HYPERLINK "http://my.nmmu.ac.za/documents/prospectus/2011_General_Prospectus.pdf" http://my.nmmu.ac.za/documents/prospectus/2011_General_Prospectus.pdf

[7] Gurpreet Dhillon and James Backhouse, "Information System Security Management in the New Millennium," *Communications of the ACM*, vol. 43, no. 7, pp. 125-128, July 2000.

[8] Micheal E Whitman, "In defense of the realm: understanding the threats to information security," *International Journal of Information Management*, vol. 24, pp. 43-57, 2004.

[9] Jan Eloff and Mariki Eloff, "Information Security Management - A New Paradigm," in *SAICSIT*, 2003, pp. 130-136.

[10] G Pavlov and J Karakaneva, "Information Security Management System in Organization," *Trakia Journal of Sciences*, vol. 9, no. 4, pp. 20-25, 2011.

[11] S Posthumus and R von Solms, "A framework for the governance of information security ," *Computers & Security*, pp. 638-646, 2004.

[12] Harold F Tipton and Micki Krause, *Information security management handbook*, 6th ed. Boca Raton, FL, USA: Auerbach Publications, 2008.

[13] Basie Von Solms, "Information security - A multidimensional discipline," *Computers & Security*, vol. 2001, pp. 504-508, 2001.

[14] Basie Von Solms and Rossouw Von Solms, "The 10 deadly sins of information security management," *Computers & Security*, no. 23, pp. 371-376, 2004.

[15] Jan Killmeyer, *Information security architecture: An integrated approach to security in the organization*. Boca Raton, FL: Auerbach Publications, 2006.

[16] Karin Hone and J H.P Eloff, "Information security policy - What do international information security standards say?," *Computers & Security*, vol. 21, no. 5, pp. 402-409, October 2002.

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

[18] ISACA. (2012) ISACA. [Online]. HYPERLINK

"http://www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx" http://www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx

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

[20] NIST SP 800-30 , *Risk management guide for information technology systems*. Washington: U.S. Department of Commerce, 2002.

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

[22] ISO/IEC 27001, *Information technology - Security techniques - Information security management system - Requirements*. Geneva: International Organization of Standardization, 2005.

[23] G J Anderson, *Fundamentals of educational research*. London: Falmer Press, 1998.