# A STRATEGY FOR MANAGING EXAMINATION SECURITY AT TERTIARY INSTITUTIONS IN SOUTH AFRICA

Short dissertation by
MARTHINUS PETRUS VAN ZYL
809602110

submitted in partial fulfillment of the requirements for the degree of

Masters in Business Administration

in the


Faculty of Management

at the

UNIVERSITY OF JOHANNESBURG

Johannesburg
October 2006

Supervisor: Prof. H.E.C de Bruyn

# CHAPTER 1

# Introduction, problem statement and objectives of the study

## 1.1 Introduction

More and more policy makers in South Africa's educational environment are focusing on the impact of digital developments on lifelong learning, electronic publishing, computer-mediated communication and the growth of virtual universities. Johnson and Scholes (1999:475) state that increased availability and quality of information can enhance an organisation's competency both by reducing the cost of processes and by improving their quality. Managers need to be clear about how these improvements in information technology should influence the way in which they manage their business processes and the benefits associated with the costs of these electronic services.



President Thabo Mbeki has stated that universities have a key role to play in improving the quality of life of all South African citizens since education is the key to unlocking each person's potential and improving the quality of life in general (Le Roux, 2005). Mbeki also emphasized that South African universities should emerge from the current process of change, ready to compete with the best institutions in the world. Mbeki asserted that change must guarantee that South Africa catches up with the best in the world in terms of the generation and use of knowledge capital to create the winning society that South Africa yearns for. It must guarantee that South Africa produces the intelligentsia who must be at the cutting edge of our process of renaissance.

Educational institutions are trying to become more competitive and efficient by transforming themselves into digital firms, where nearly all core business processes and relationships with customers are digitally enabled. The associated metamorphosis of historically paper based assessment processes is putting increasing pressure on institutions to find easier and more cost effective ways of designing, securely transferring and storing exam papers and memoranda, as well as conducting exams and assessing learners.

There are also different views on how to use electronic enhancements to improve business processes. Roberts and Chambers (2001:21-25) argue that enhanced learning and increased access to information also increase potential threats to creativity, academic freedom, teaching and research quality. The possibility of using information systems to enhance education should thus be explored with a view to enhancing learning and improving teaching practices without sacrificing the integrity or quality of service providers.



Information systems, according to Laudon and Laudon (2002:6-7), are a set of interrelated components that collect (or retrieve), process, store and distribute information to support decision making, co-ordination, and control in an organization. The digital firm is one in which nearly all the organization's significant business relationships with customers, suppliers and employees are digitally enabled and mediated. The secure use of information systems to enhance both service delivery and turn around time in the examination section of tertiary institutions is, firstly, essential for survival in this day and age and, secondly, unavoidable when it comes to transformation into a digital firm in order to compete for local and global market share.

## 1.2 Problem statement

Educational institutions are trying to become more competitive and efficient by transforming themselves into digital firms, where nearly all core business processes and relationships with customers are digitally enabled. The associated metamorphosis of historically paper based assessment processes is putting increasing pressure on institutions to find easier and more cost effective ways of designing, transferring and storing examination papers and memoranda, as well as conducting examinations and assessing learners.

Security, as defined by Laudon and Laudon (2002:438), is the policies, procedures and technical measures used to prevent unauthorized access, alteration, theft or physical damage to information systems. Security can be promoted using an array of techniques and tools to safeguard information. In higher education institutions, the security of student marks is one of the most sensitive issues that needs to be addressed as well as the safeguarding of unwritten examination papers. Nothing would harm an institution more than acknowledging that the security of their systems has been breached resulting in unauthorised mark changes or the leaking of examination papers.



South African tertiary education service providers lack a proper strategy for managing examination security, particularly when it comes to the implementation and use of information technology to drive secure electronic business processes.

## 1.3 Research objectives

The primary objective of this study is to investigate the level of technology implemented to ensure secure business processes to support examinations in tertiary institutions in South Africa. This study will also identify risk factors and recommend operational strategies to improve and securely manage electronic business processes.

Roberts and Chambers (2001:156) argue that institutions must recognize and accept the need to review traditional methods of quality assurance and perhaps even re-think what they regard as quality. Recommendations drawn from the research will enable South African institutions to implement a healthy, competent and supportive information systems structure to support secure examinations and, ultimately, quality assurance.



To execute the primary objective the following additional objectives have to be attained:

- The development of operational guidelines to streamline the business process required for implementing and maintaining secure information systems in the examination section of South African higher education institutions.
- Recommendations will be formulated in order to provide guidelines for institutions that want to implement or review the electronic business process security that supports their examination functions.

## 1.4 Research design and methodology

The research design and methodology of this study consists of primary and secondary research.

### 1.4.1 Secondary research

The review of the nature and background of information systems security and general information concerning operational strategies is based on a study of a wide variety of literature. This includes recent articles sourced from the internet, articles published in academic and non-academic journals and magazines, as well as books published by specialists in their field of study.



Hart (1998:13) defines a literature review as the selection of available documents (both published and unpublished) which contain information, ideas, data and evidence written from a particular standpoint in order to fulfill certain aims or express certain views on the nature of the topic and how it is to be investigated. The literature review further includes an effective evaluation of these documents in relation to the research being proposed.

The importance of a literature review therefore, is to establish the most widely accepted empirical findings pertaining to the research topic and to identify available instrumentation that has proven validity and reliability.

The literature available for this type of study is limited (because of the focus) and is thus based on international studies and key operational concepts. Nonetheless, it will still provide valuable viewpoints and critical guidelines.

### 1.4.2 Primary research

Zikmund (2003:369) states that the process of sampling involves any procedure using a small number of representatives of the whole population in order to draw a conclusion about the whole population. All higher education institutions in South Africa will be given the opportunity to complete the questionnaire, and only senior managers or policy makers within the examination domain will be allowed to complete and comment on the questionnaire.

A questionnaire will be used to collect information and gather the relevant data from external parties. Information will be collected from key people at tertiary institutions who have policymaking influence or managerial control and who have in-depth knowledge of the operational examination process of the institution.



Electronic questionnaires will be distributed and collected to harness the convenience and speed of e-mailing documentation between parties. Primary considerations in the design of the questionnaire will be the seven principles of questionnaire design identified by Dillon, Madden & Firtle (1993:303).

The validity and reliability of this study will be supported by the triangulation of the findings through cross-referenced findings in case studies, the questionnaire and literature review. The data to be collected for this study will be primarily qualitative with a small portion of quantitative data that will be analysed.

## 1.5 Outline of study

Chapter two investigates how information systems are transforming tertiary institutions and the management of examinations. Advances in information technology have fostered the emergence of e-learning and virtual universities across the globe. This, in turn, has created unprecedented opportunities for enhancing study aids and crossing the physical barrier of instruction. However, in turn this has created a void relating to the technology used to administer examination processes like submitting examination papers and marks electronically after assessments securely.

Chapter three identifies risk factors within the examinations domain. These risk factors include issues such as academics and administrative departments utilising e-mail technology to send and receive examination question papers. This chapter considers the use of information systems that have transformed tertiary institutions and, more specifically, the risks associated with the use of electronic business processes for the management of examinations.



Chapter four focuses on formulating operational strategies based on the data from this studying order to assist examination managers to manage the security needs of the examination domain at tertiary institutions. The primary aim of this chapter is not to criticize operational practices in the higher educational arena, but rather to inform policy makers about the impact of using information systems and the security needs associated with such system.

## 1.6 Closure

The objective of this chapter was to justify the research and emphasise the problem statement. The preliminary research conducted shows that a strong demand for a study of this nature exists. The benefits of this study will include the provision of clear guidelines to higher educational institutions on how well they have implemented electronic security in the examination function and to what extent it is possible to enhance the secure electronic flow of business processes within this function.

Institutions will be able to assess their security needs and strategise according to a proposed best practice framework for the handling of all tasks concerning the electronic compilation of examination papers, the submission of examination marks electronically and having secure access to previous examination papers and memoranda. Another aspect of this study is the assessment of sensitivity about the security needs in examination departments in the South African educational sector.



An Examinations Manager will be able to draw clear conclusions about whether the department has possible shortcomings regarding electronic security or if the department needs to assess the current situation to determine whether it needs to implement additional electronic solutions to enhance and expedite the processes.

# Chapter 2
# Information systems and the management of examinations

## 2.1 Introduction

Luftman (2004:2) states that information technology is an important and necessary component of a successful organization. Advances in information technology have encouraged the emergence of e-learning and virtual universities across the globe. This, in turn, has created unprecedented opportunities for developing study aids and crossing the physical barrier of instruction. However, in turn, this has created a void relating to the technology used to administer examination processes like submitting examination papers and marks electronically after assessments securely.



The critical challenge for institutional leaders today is how to manage security amidst the phenomenal advances in technology. Specifically, the critical challenge will be the ability to adapt and implement new technologies to support institutions.

This chapter aims to consider the use of information systems that transform tertiary institutions and, more specifically, convert the management of examinations into an electronic business.

## 2.2 The internet

According to Shelly, Cashman & Vermaat (2005:68) the internet, also called the net or World Wide Web is a worldwide collection of networks that link millions of businesses, government agencies, educational institutions and individuals. Today, more than one billion users around the world connect to the internet for a variety of reasons. The acceptance and increasingly dominant use of the internet allows in formation to be spread almost instantaneously and more widely than ever before.

The benefits of using the internet, according to Laudon and Laudon (2002:280-281), include its global connectivity, ease of use, low cost and the ability to create interactive multimedia capabilities. By using internet technology, organizations can reduce communication and transaction costs, enhance coordination and collaboration, and accelerate the distribution of knowledge. The use of internet technology in managing examination information has drastically re-shaped office and support structures such as the equipment and staffing required and the way in which policy makers share information.



Many institutions presently rely on the internet and related technologies to inform students of all examination related information. Many even allow for the electronic downloading of past examination question papers. Today the internet is the primary preferred medium of communication between an institution and students, because of its ease of use, speed in disseminating information and the ability to download information anywhere in the world.

Luftman (2004:6) states that the internet has enabled communications that are independent of time and place. The ubiquity of the internet and its ability to transmit and receive rich communication that can include documents, sounds, video and links to internet sites, serves to extend the nature of communications well beyond that of the traditional telephone. When one looks at the business processes within the examinations domain, this is where information technology has advanced the most with the use of web technology to enhance communication between students (clients) and the institution. Internet applications are being increasingly used to develop a secure web portal where academic staff can log on (with a username and password) to enquire about their student statistics, population dynamics and payment status. This portal can also allow for the secure submission of electronic examination question papers and the submission or finalisation of term and examination marks electronically from the comfort of their home or office.



According to Luftman (2004:8) the integration of the internet and internal information systems (the linkage of business systems to a public network) creates security concerns. Organisations must protect important data from external parties who can gain access by exploiting vulnerabilities in systems. Student information systems or Enterprise Resource Planning (ERP) systems are used to publish information like examination timetables and examination results on tertiary institutions' websites for students to access around the globe. While this makes the information accessible worldwide at the push of a button, it also creates a security concern.

The explosive growth of internet use by businesses and individuals has been accompanied by rising reports of internet security breaches. Laudon and Laudon (2002:435) explain that the main concern arises from unwanted intruders, or

hackers, who use the latest technology and their skills to break into supposedly secure computers or to disable them. A hacker is a person who gains unauthorized access to a computer network for profit, criminal mischief or personal pleasure. Hacker break-ins can harm businesses in many ways. Some malicious intruders have planted logic bombs, Trojan horses and other software that can hide in a system or network until they are activated at a specified time. Laudon and Laudon (2002:438) define security as the policies, procedures and technical measures used to prevent unauthorized access, alteration, theft or physical damage to information systems. Security can be promoted with an array of techniques and tools designed to safeguard computer hardware, software, communications networks and data.

Electronic processes, such as the internet, that are used thus need to be secure and controlled because such processes are basically part of the service chain of the examinations department. Security measures to safeguard and control this electronic medium of distributing information need to be discussed in depth with the relevant policy makers or examination managers.



## 2.3 Short message service (SMS)

According to Shelly, Cashman & Vermaat (2005:463) a mobile device with text messaging, also called SMS (short message service), capability allows users to send and receive short text messages on a telephone. Most text messaging services limit messages to a specific number of characters, usually fewer than 300 characters. Short message services typically provide users with several options for sending and receiving messages: mobile telephone to mobile telephone, mobile telephone to e-mail (send the message from your mobile

phone to an e-mail address anywhere in the world) or Web to mobile (send the message from a web site to a mobile device).

In the examinations domain, electronic business processes also encompass the use of SMS technology to allow the spread of examination information to a broader spectrum of technology users. Educational institutions can also utilise the strengths of SMS technology to provide information to their students and staff. Students or learners can now, upon disclosure of their cell phone numbers, receive frequent updates on examination information such as the dates and times of examinations and even examination results as they become available. This availability relieves students of physically traveling to institutions to get their examination timetable or results, giving them a lot more flexibility when it comes to time management and travel costs. SMS technology can now be integrated with the institution's communication strategy to communicate more effectively, faster and on a more personal note with students or staff. This new distribution method of sensitive student specific information thus also needs to be securely controlled from an examination management point of view in order to ensure data integrity and access to information.



Shelly, Cashman & Vermaat (2005:464) state that several schools have banned student cellular telephones, claiming that they disrupt classes and are sometimes used for illegal activities, such as sending SMS's to each other with answers to test questions. Students have also been caught using camera enabled cellular phones to take pictures of tests and forwarding the images to students scheduled to take the test at a later time. Therefore, the use of this technology also needs to be closely monitored and the security risks associated with it re-assessed from time to time as the technology changes.

Designing systems that control procedures need to be neither over controlled nor under controlled. Although most security breaches and damage to information systems still come from organizational insiders, according to Laudon and Laudon (2002:435), security breaches from outside the organization are increasing because firms using electronic communication are open to outsiders via the internet.

It is difficult for organizations to determine how open or closed they should be in order to protect themselves adequately. If a system requires too many passwords, authorizations or levels of security to access information, the system will not be used. Controls that are effective, but which do not prevent authorized individuals from using a system, are difficult to design.

According to Laudon and Laudon (2002:441) in order to minimize errors, disaster, interruptions of service, computer crime and breaches of security, special policies and procedures must be incorporated into the design and implementation of information systems. The combination of manual and automated measures that safeguard information systems and ensure that they perform according to management standards is termed controls. Electronic security related issues and the lack of technology focus when it comes to examination departments' electronic advancement, have only allowed small advances such as the use of SMS technology in a mostly manual operational environment that requires exceptional security controls.

The ultimate aim of transforming manual processes into electronic processes to enhance communication within the examinations domain using technology like SMS will rely on a stable and secure electronic environment. Chen (2001:54) points out that a crucial element allowing electronic commerce over the internet

has been the development of software to ensure security of transactions. New software and standards to improve the security of transactions are being developed all the time. This is why this technology needs to be closely monitored for changes and security threats that might be created through rapid improvements.

.

## 2.4 Electronic mail (e-mail)

Shelly, Cashman & Vermaat (2005:92) defines that electronic mail (e-mail) as the transmission of messages and files via a computer network. Laudon and Laudon (2002:186) describe e-mail as a tool that is used for the computer-to-computer exchange of messages and note that it is an important tool for communication and collaborative work. E-mail was one of the original services on the internet, enabling scientists and researchers working on government-sponsored projects to communicate with colleagues in other locations. Today, e-mail is a primary communication method for both personal and business use.



Nowadays e-mails are widely accepted as the preferred medium of business communication because of the speed of delivery and worldwide availability. The technology is available and is being utilised to expedite service delivery in the examination domain by enhancing services in areas like examination queries from students and academics and general business communication. However, e-mail technology could be used for much more in this domain, for instance the electronic submission of examination question papers via e-mail, if security concerns are addressed.

Presently many institutions still require academics to personally travel great distances to submit their examination question papers in hard copy format. Why

do so many institutions find it difficult to expedite the submission of examination question papers electronically utilising e-mail? Allowing the use of electronic mail (e-mail) to submit examination question papers and memoranda must not only be controlled with very strict security measures, but should also utilise a combination of electronic and manual controls, for instance password protection, verifying the author and using a secure network.

Luftman (2004:166) points out that the majority of businesses today do not have a company-wide security policy, yet all companies that have an intranet, local area network (LAN) or a website are subject to a number of potential security threats. Some of the better-known security issues are unauthorised access to confidential data, illegal use or monitoring of e-mail systems and virus attacks. Thus, it is essential to create a controlled environment, where examination processes can be electronically enabled while simultaneously having the highest regard for security and controls.



Controls, according to Laudon and Laudon (2002:441), consist of all the methods, policies, and organizational procedures that ensure the safety of the organization's assets, the accuracy and reliability of its accounting records, and operational adherence to management standards. In the past, the control of information systems (which includes secure e-mails) were treated as an afterthought, addressed only towards the end of implementation, just before the system was installed. Today, however, organizations are so critically dependent on services like e-mail that vulnerabilities and control issues must be identified as early as possible.

The heightened vulnerability of electronic data has created special concerns for the policymakers who manage examination processes. While electronic business

operations do add to the overall enhancement of business processes, they also need to be extra secure and extra stable in the case of examinations. There should also be a clear disaster recovery plan in place. Laudon and Laudon (2002:438) state that a disaster recovery plan is a plan for running the business in the event of a computer outage. This includes organizational procedures as well as backup processing, storage and database capabilities.

A balance needs to be found between utilising advances in technology, for instance e-mail, to enhance communication and administration within the examination department without compromising security and quality. Thus focusing on system processes that are neither over controlled nor under controlled will be the only way forward.

## 2.5 Closure



In too many instances, education policymakers view business processes and changes in these processes as just another top-down reform, divorced from the needs and realities of the administration of examinations. Moreover, they pay too little attention to the effective development and enhancement of a secure administrative process that is driven by technology.

Electronic business processes require organizations to be simultaneously both more open and more closed. To benefit from electronic processes or any other digital process, institutions need to be open to customers such as students and to employees such as academics. The use of information technology in the examination department of educational institutions requires a new security culture and infrastructure that allows institutions to straddle a fine line between

supporting secure business processes and providing quality and stable electronic educational services.

There is a simple conclusion to be drawn from the above: electronic policies and procedures seeking to improve the quality of examination administration must provide more help and less insecurity.

# Chapter 3

# The identification of risk factors within the examination domain

## 3.1 Introduction

This chapter identifies risk factors linked to operational procedures and associated with the general management of examinations at tertiary education institutions in South Africa. The focus is primarily on global technological advances and the security requirements necessary to utilise these advancements effectively.



Johnson and Scholes (1999:498) state that a learning organisation is capable of benefiting from the range of knowledge, experience and skills of individuals by developing a culture that encourages mutual questioning and challenge around a shared purpose or vision. The organisation then becomes capable of taking a holistic view of its environment rather than being reliant on partial, filtered information from its various functions. This forms the basis of a continual evaluation of operational needs and strategies within both the institution and the examination domain to determine the security needs and risk factors that need to be addressed when changing processes.

This study harnessed the knowledge of operational policy makers within all the higher education institutions in South Africa by means of an electronic questionnaire. The questionnaire was sent to the Examination Department's

Manager or Director of all the higher educational institutions in South Africa. The questionnaire included three sections all of which had to be completed.

Section A requested personal and operational information of the policymaker for example his/her age, educational level, experience and the use of technology at the institution. This section was designed to determine the level of experience in the department and the operational use of technology to administer examinations securely at each institution.

Section B elicited the institution's perception of what would be important for the examinations department at an ideal institution from a security point of view compared to the current situation at the institution. Here we also assessed the sensitivity of more specific risk areas such as mark audits and administrator passwords for computers used in the examinations department.



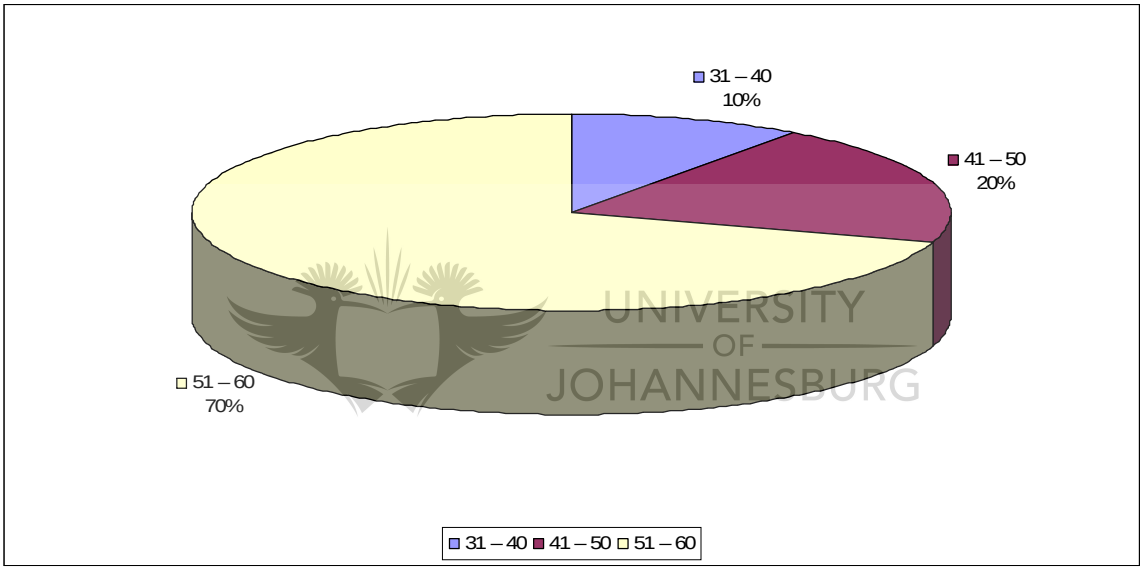
Section C evaluated the relationship between the examinations department and the Information Technology (IT) or Information Systems (IS) department and included some open-ended questions relating to experiences and risk factors. This section was designed to ascertain whether specific security risks have been identified or addressed by policymakers in the past or have more recently been identified because of technological advances or changes.

## 3.2 Policy makers

When looking at the span and control of the examinations domain one needs to correlate the responsibilities with the demographics of the educational sector to try to define a model policy maker. Policy makers can be defined as examination department managers or directors who are responsible for both the overall administrative duties and for the enforcement of assessment policies and

procedures. When considering the age of policy makers or examination managers (see graph 3.1), this survey concluded that 20% of them are between the ages of 41 and 50 and 70% are aged between 51 and 60 years. This highlights the fact that senior (in terms of age) managers drive South African institutions. The rest of the managers (10%) are between the ages of 31 and 40 years.

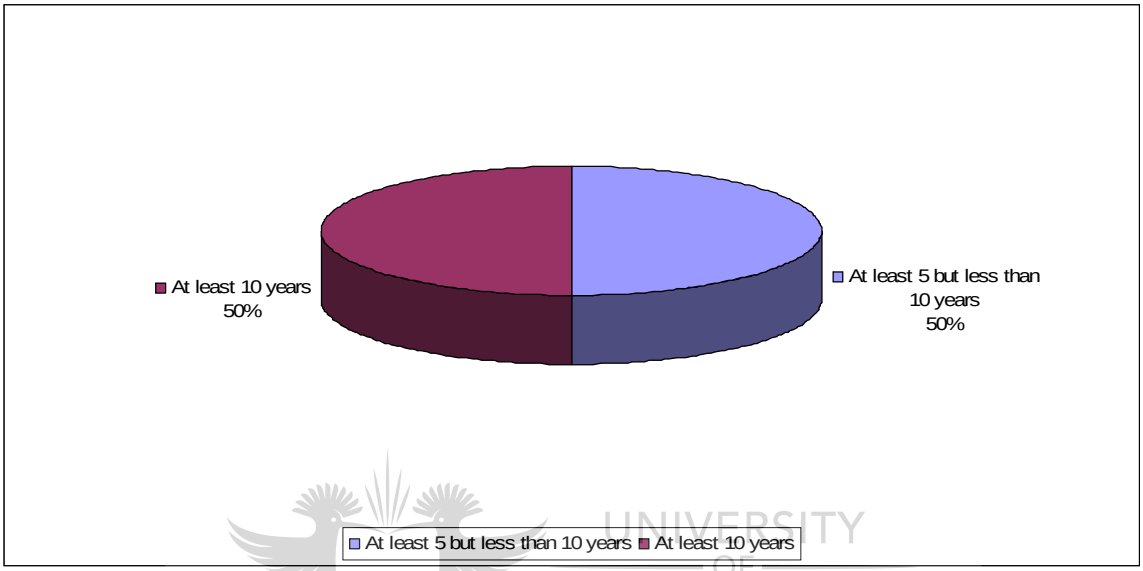
Graph 3.1 The age of Examination Managers (in years).




Analysis of operational experience in the examination department (see graph 3.2) also concluded that 50% of the managers had been managing examinations for between 5 and 10 years while the remaining 50% had been doing o for more than 10 years. This highlights the fact that examinations in higher education institutions in South Africa are managed by senior and experienced staff members, taking their age and experience into consideration. Analysis of the gender composition (see graph 3.3) of the managers in this study showed that policy makers in the examinations department in higher education institutions are

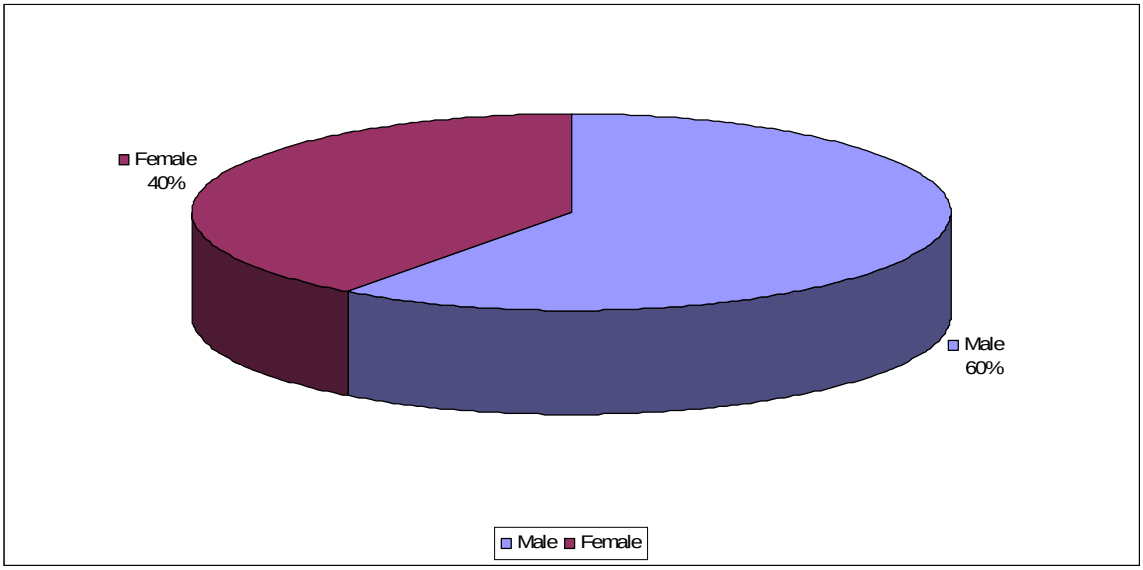
balanced in terms of gender, with 60% of the examination managers being male and 40% being female.

Graph 3.2 The experience of Examination Managers (in years).



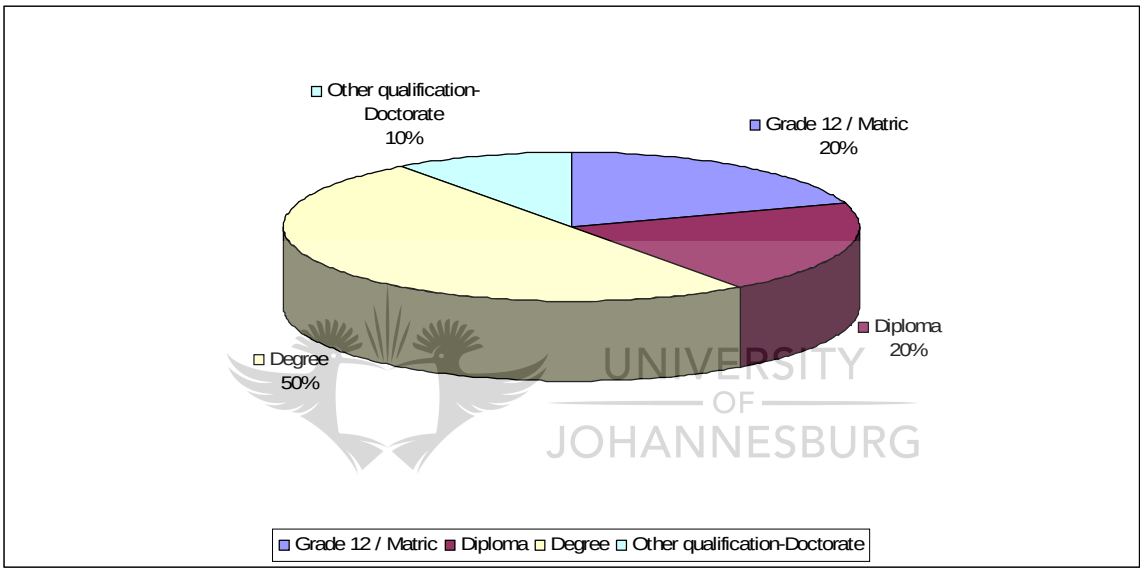



Graph 3.3 The gender of Examination Managers.



The highest educational level achieved (see graph 3.4) found that 20% of the managers had only a grade 12 or matric, 20% had obtained a diploma, 50% had gained a degree and 10% had received a doctorate degree. This substantiates the assertion that examination managers are mostly senior managers in terms of their age, their experience and their education, which enhances their skills.

Graph 3.4 The educational level of Examination Managers.




The demographical information will be used in the data analysis to determine how involved, skilled and suitable examination managers are in the management of technological security in their environment.

## 3.3 System security and support

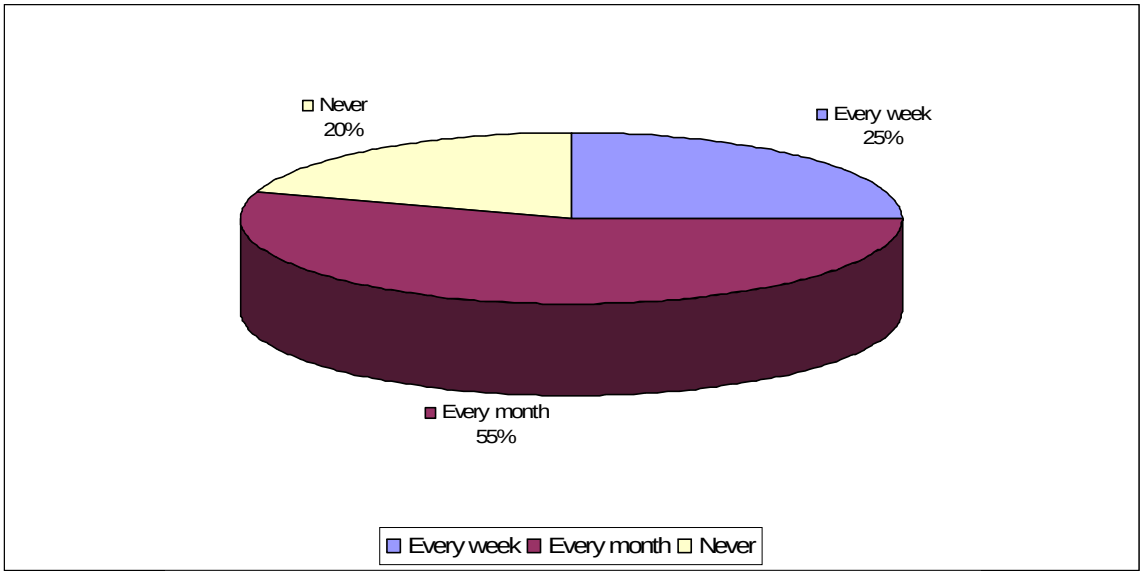
One of the biggest problems with system security is the human factor. The fact people use personal words or phrases as passwords or that they write down the password on a piece of paper next to their PC constitutes significant security risk.

Most people do not understand the risk they pose to their company because of the lack or misuse of system passwords.

One positive aspect is the fact that 100% of the respondents said that the PCs used for examination purposes are password protected. But the follow up question about how often they change the passwords (see graph 3.5) ascertained that only 25% changed the password weekly, 55% changed it monthly and 20% reported never changing the password. One could believe that strong controls are in place since 80% of institutions change their passwords within 30 days. However, the remainder of the institutions (20% of institutions) which never change passwords may be the institutions that receive negative publicity because of a major court case relating to stolen qualifications or fraudulent marks given to students.

It is important to note that the quality of the passwords used at institutions was not determined. The research merely established whether passwords are used and whether they are changed regularly.

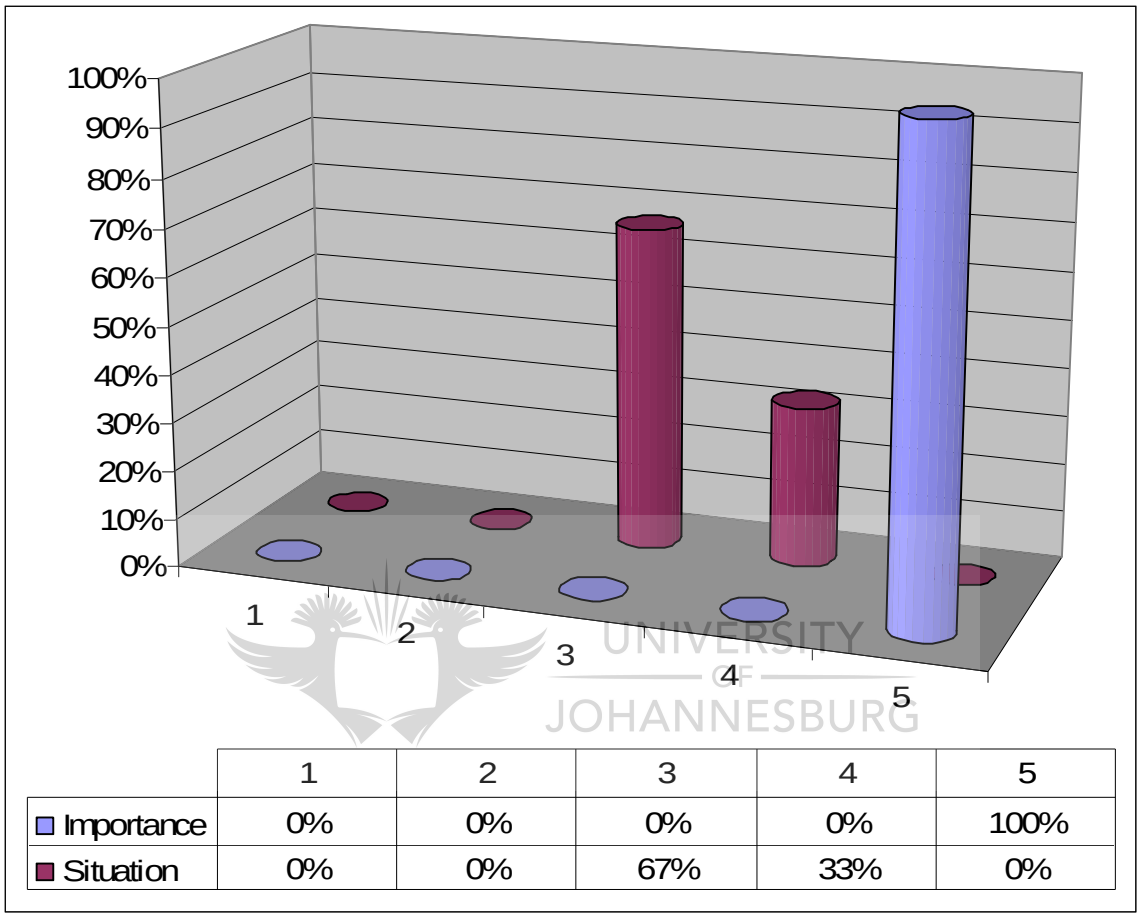
Graph 3.5 The frequency of password changes in the examination domain.




Another important aspect that was investigated in this study is the relationship between how important certain aspects are to institutions compared to their internal situation at this moment. This identified critical shortcomings and highlighted areas of concern which institutions feel they must improve.

Respondents were asked to rate the importance, ranging from 1 (not important) to 5 (extremely important) of updating local PC and network passwords at an ideal institution. The research found that 100% of the institutions believed that frequent updating of passwords is extremely important (see graph 3.6). However, 67% of the institutions rated themselves as being average and 33% as being above average in this regard. This suggests that many institutions feel that they need to strengthen their security relating to password protection.

Graph 3.6 The frequency of PC and network password updates in the examinations domain.




| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Importance | 0% | 0% | 0% | 0% | 100% |
| Situation | 0% | 0% | 67% | 33% | 0% |

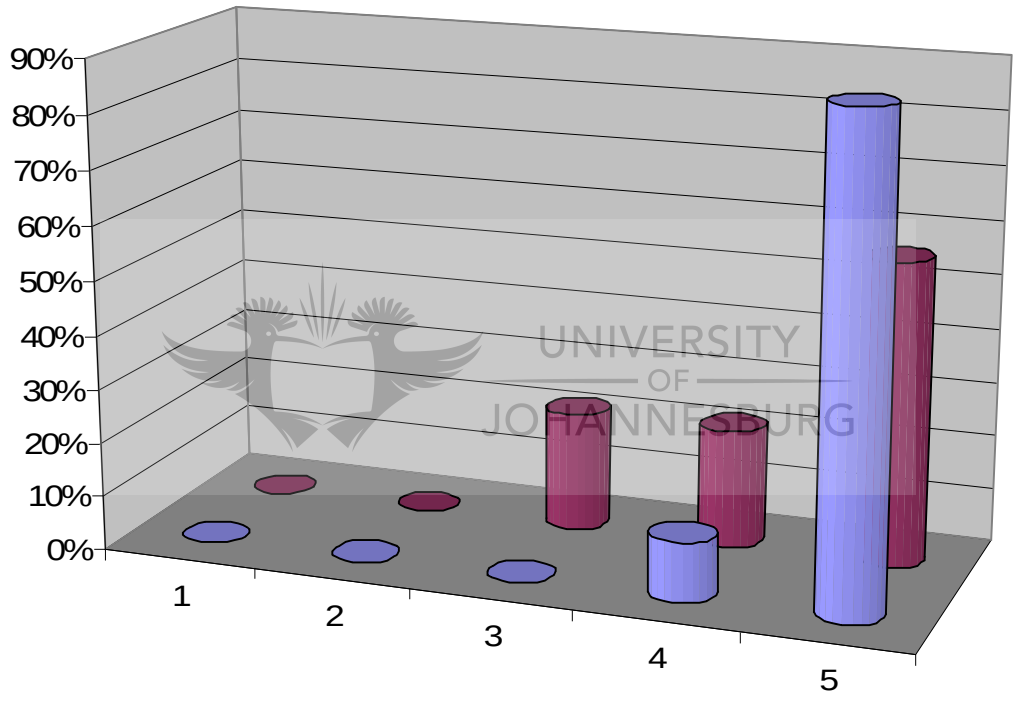
Importance (at an ideal institution) 1 = not important, 2 = less important, 3 = average importance, 4 = very important, 5 = extremely important.

Situation (at all the institutions) 1 = very poor, 2 = poor, 3 = average, 4 = good, 5= excellent.

Another aspect relating to system security investigated by the research was whether institutions feel that network and local PC access is strictly controlled (see graph 3.7). This assessed the security awareness measured by the adequacy or lack of internal security controls put in place by IT or IS departments in examination departments. Eighty nine percent of institutions believed network and local PC access control to be extremely important (5) while 11% stated that it

is very important (4). However, only 56% of the institutions rated the access control as being excellent (5) while 22% felt that it is average (3) and the remaining 22% thought that it is above average. This indicates that institutions feel they can improve their network and PC access.

Graph 3.7 The control of local PC and network access in the examinations domain.






| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Importance | 0% | 0% | 0% | 11% | 89% |
| Situation | 0% | 0% | 22% | 22% | 56% |

Importance (at an ideal institution) 1 = not important, 2 = less important, 3 = average importance, 4 = very important, 5 = extremely important.

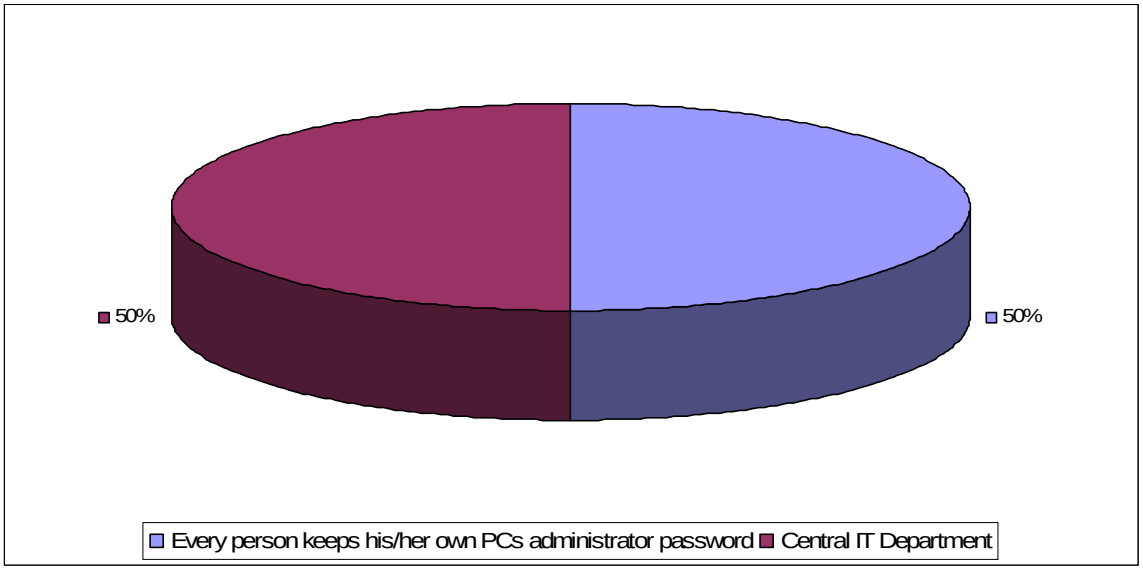
Situation (at all the institutions) 1 = very poor, 2 = poor, 3 = average, 4 = good, 5= excellent.

Every PC is set up with an administrator account and a user account, which is used to log onto the machine. With the password for the administrator account of a PC one can gain access to everything on it and copy, delete or even view what is happening on that machine remotely at any time. Thus, another security aspect that needs to be investigated is who has access to the administrator passwords of PCs in the examination department. In other words, who keeps the administrator passwords to the PCs used to type exam papers and to capture exam marks?

Fifty percent of respondents stated that the institution allows the examination department's staff to keep the administrator password to their PCs (see graph 3.8). This would be the best security arrangement if the password quality is adequate and if updates are done regularly. However, the remaining 50% stated that the information technology (IT) or information systems (IS) department keeps their administrator passwords, which maintains the PCs.

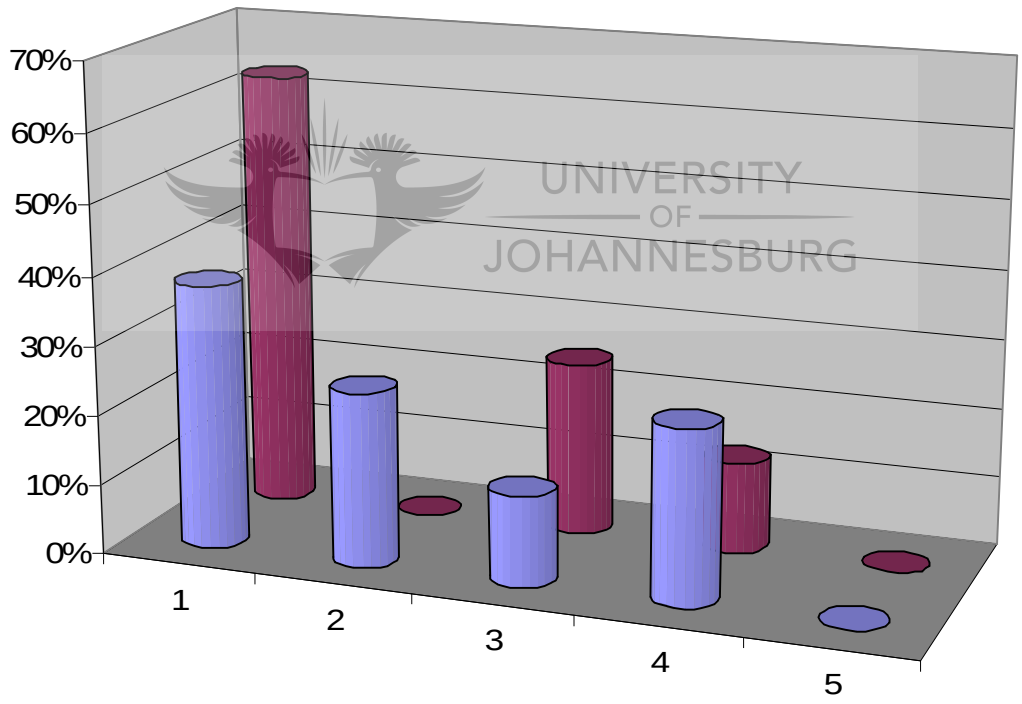


Graph 3.8 Who keeps the administrator password?



Results of the importance against situation comparison (see graph 3.9) show that 63% (38% = not important and 25% = less important) of institutions feel that their IT department does not need access to the administrator passwords of their PCs. In contrast, however, 63% of institutions reported a very poor situation reflecting that most of the examinations departments do not have control over their administrator passwords or access to examination PCs.

Graph 3.9 Does the IT department need access with the administrator password to the PCs used to administer examinations?






| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Importance | 38% | 25% | 13% | 25% | 0% |
| Situation | 63% | 0% | 25% | 13% | 0% |

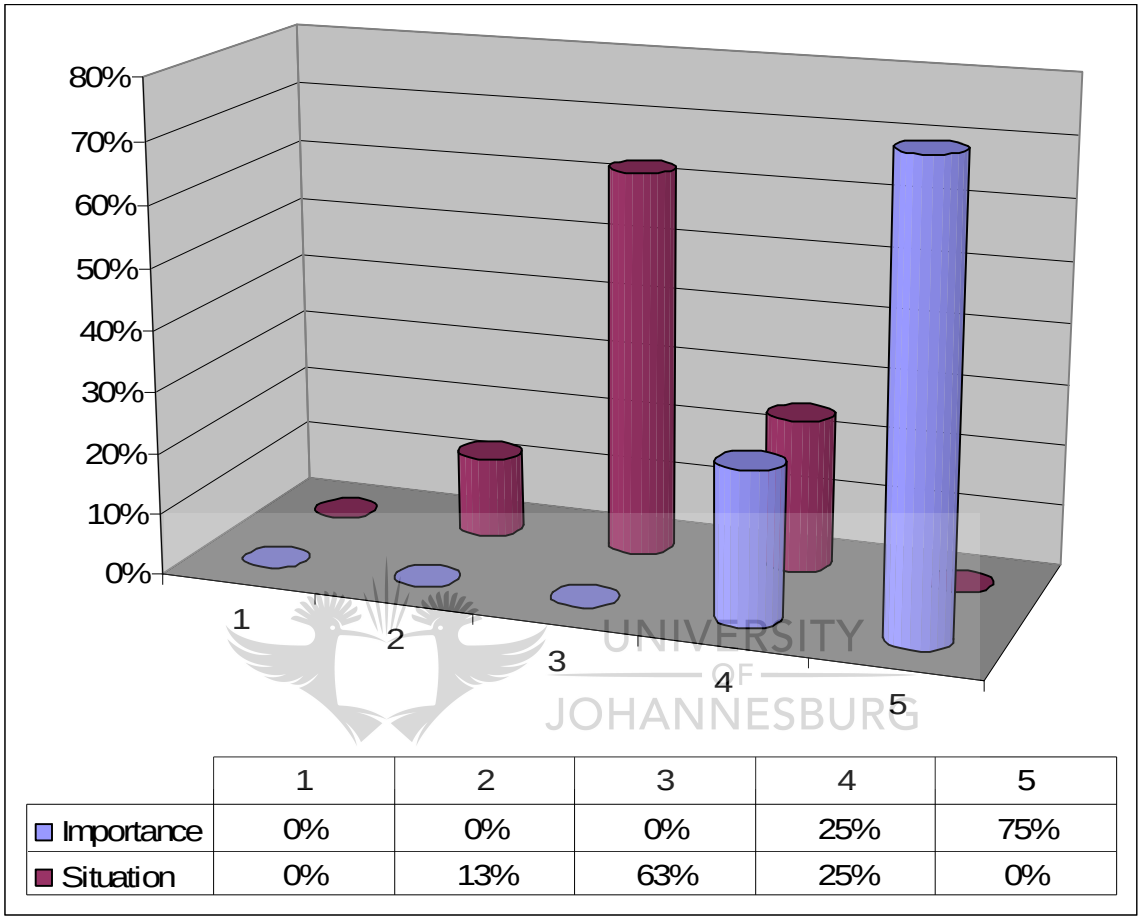
Importance (at an ideal institution) 1 = not important, 2 = less important, 3 = average importance, 4 = very important, 5 = extremely important.

Situation (at all the institutions) 1 = very poor, 2 = poor, 3 = average, 4 = good, 5= excellent.

From an IT or IS manager's point of view, keeping the administrator password centrally is a good idea since they are responsible for maintaining PCs and assisting staff who have locked themselves out of their own PCs when they forget their passwords. Nevertheless, from an examinations manager's point of view this arrangement needs to be looked at very critically because it means that there is another vulnerability to manage.

The response from institutions relating to the IT department's assistance in the management of examination system vulnerabilities indicated that 75% consider this aspect to be extremely important while the remainder 25% see it as very important. However, the situation analysis shows that 65% consider their situation to be average while 13% even reporting it as being poor (see graph 3.10).

Graph 3.10 Your IT department warns and aids you in terms of technological vulnerabilities and security threats.




| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Importance | 0% | 0% | 0% | 25% | 75% |
| Situation | 0% | 13% | 63% | 25% | 0% |

Importance (at an ideal institution) 1 = not important, 2 = less important, 3 = average importance, 4 = very important, 5 = extremely important.

Situation (at all the institutions) 1 = very poor, 2 = poor, 3 = average, 4 = good, 5= excellent.

Technical information about technological vulnerabilities should thus be communicated to the policy makers in the examination domain to enable them to plan and critically evaluate the need for and risk of operational requirements utilising the technology (e.g. e-mailing examination papers).

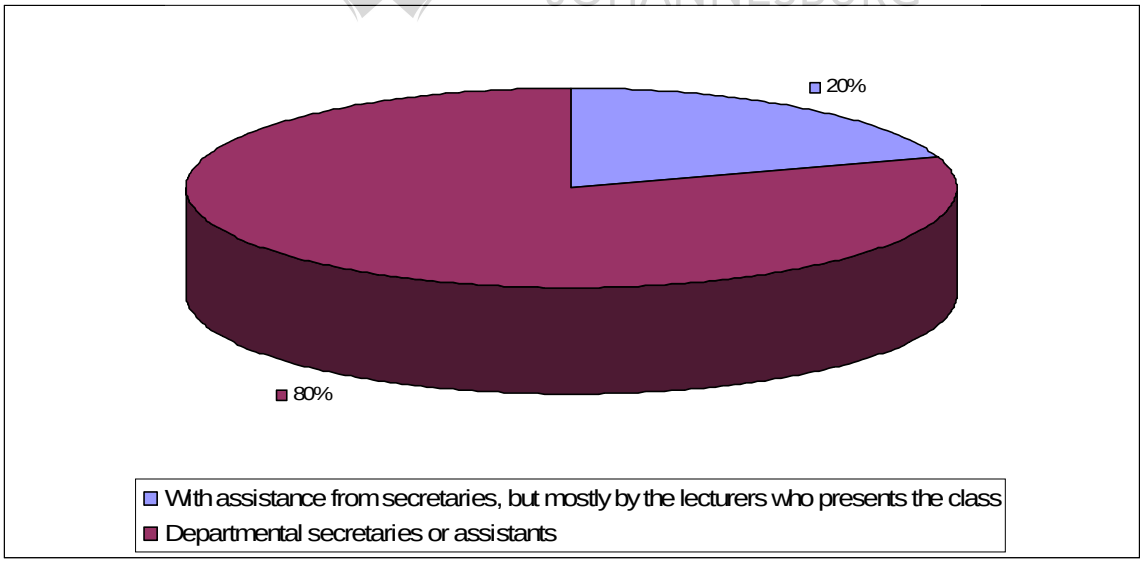
## 3.4 Preparing and reproducing examination papers

Critical care needs to be exercised when preparing and reproducing examination papers from a policy formulation point of view. This process lends itself to much vulnerability such as e-mail systems and storing examination papers on PCs or servers.

The first point of contact is the person who types or prepares the examination papers. Eighty percent of the institutions stated that departmental secretaries or assistants are involved in the typing of examination question papers (see graph 3.11) while only 20% reported that the lecturer prepares the question papers with the assistance of secretaries.



Graph 3.11 The typing of examination papers is done by whom?

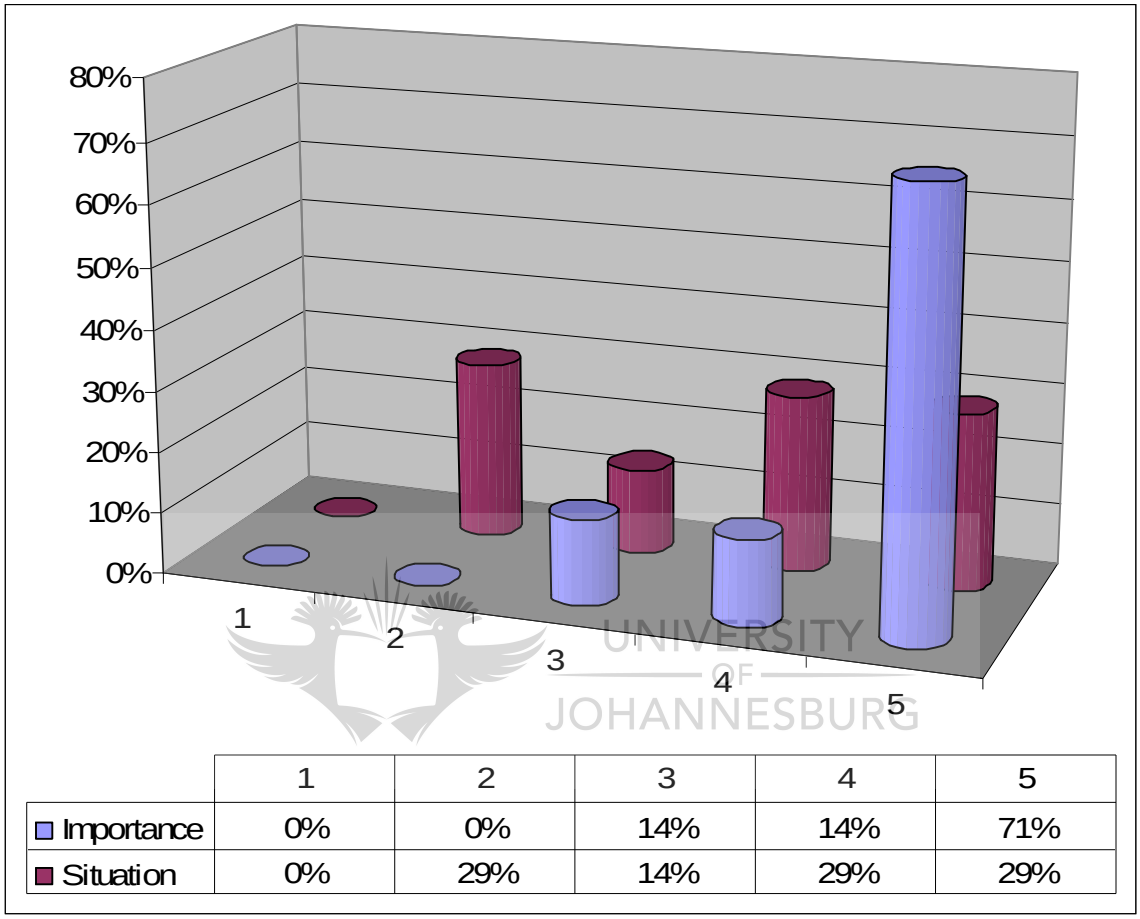



Another aspect, as mentioned above, is the e-mailing of examination question papers between the parties involved with the examination, for example,

submitting the question papers electronically via e-mail to the examination department. One critical aspect would be the password protection of documents if they would in any way be compromised if opened by the wrong person.

Respondents in this study stated that, overall, 85% of them deem this extra security measure (password protecting the e-mailed document) as being very or extremely important (14% deem it to be very important and 71%, extremely important see graph 3.12). In terms of their current situation, 29% of institutions believe that they manage this situation well, while another 29% believe that their management of password protection is excellent.

Graph 3.12 Before examination papers are e-mailed, do they need to be password protected?



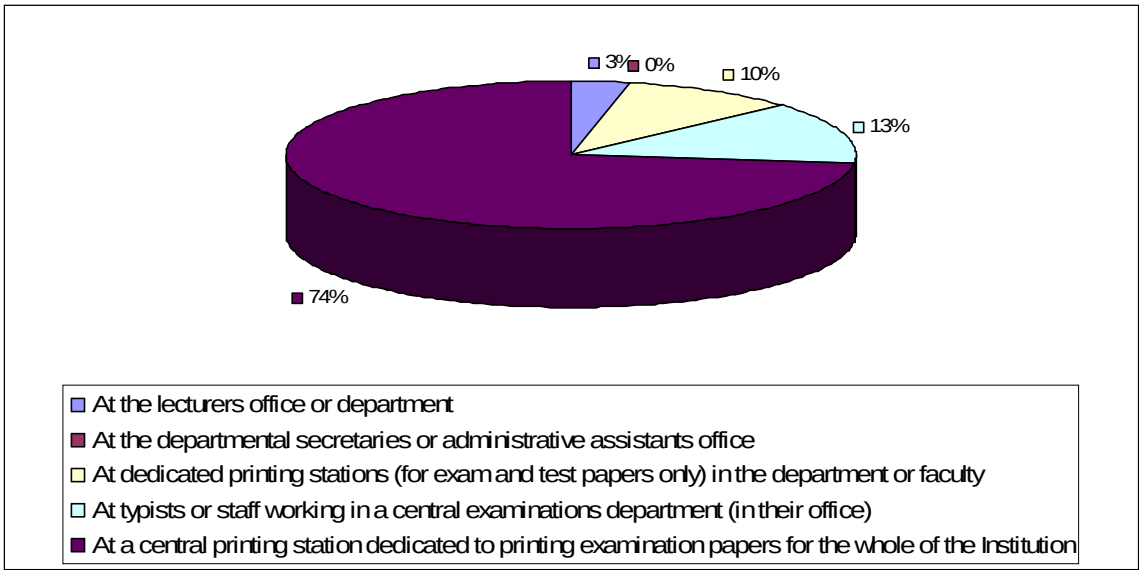

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Importance | 0% | 0% | 14% | 14% | 71% |
| Situation | 0% | 29% | 14% | 29% | 29% |

Importance (at an ideal institution) 1 = not important, 2 = less important, 3 = average importance, 4 = very important, 5 = extremely important.

Situation (at all the institutions) 1 = very poor, 2 = poor, 3 = average, 4 = good, 5= excellent.

Another positive aspect that was noted was the fact that 73% of institutions use a central printing station that is dedicated to the printing of examination question papers for the whole institution (see graph 3.13).

Graph 3.13 The reproduction of examination papers.




## 3.5 Safeguarding of examination papers

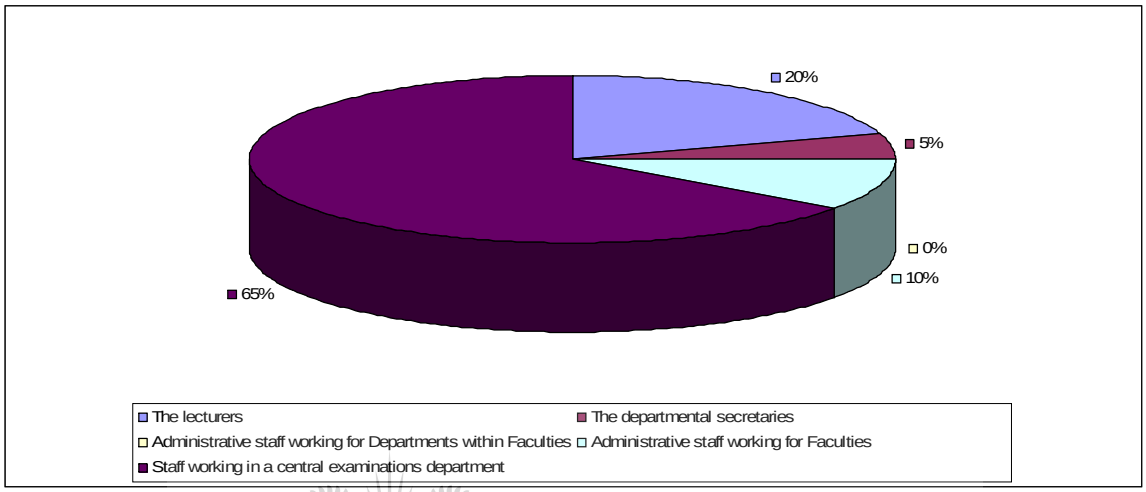


Examination papers should be one of the most securely guarded aspects of the examinations department. This is why the examination department has to monitor and control the storage of examination papers very closely in order to ensure their integrity. Two aspects need to be considered when administering this function. The one consideration is the electronic storage of the question papers and the other is the storage of the reproduced question papers in paper format (i.e. copied and ready to be written by the students).

When considering the storage of the paper copies of examination papers, 65% of institutions reported that they store their examination papers centrally with examination staff working for the examinations department. In 20% of institutions the question papers are stored by the lecturers and in 10% of institutions

administrative staff working in the faculties are responsible for the storage of examination papers (see graph 3.14).

Graph 3.14 The safeguarding of examination papers before they are written.

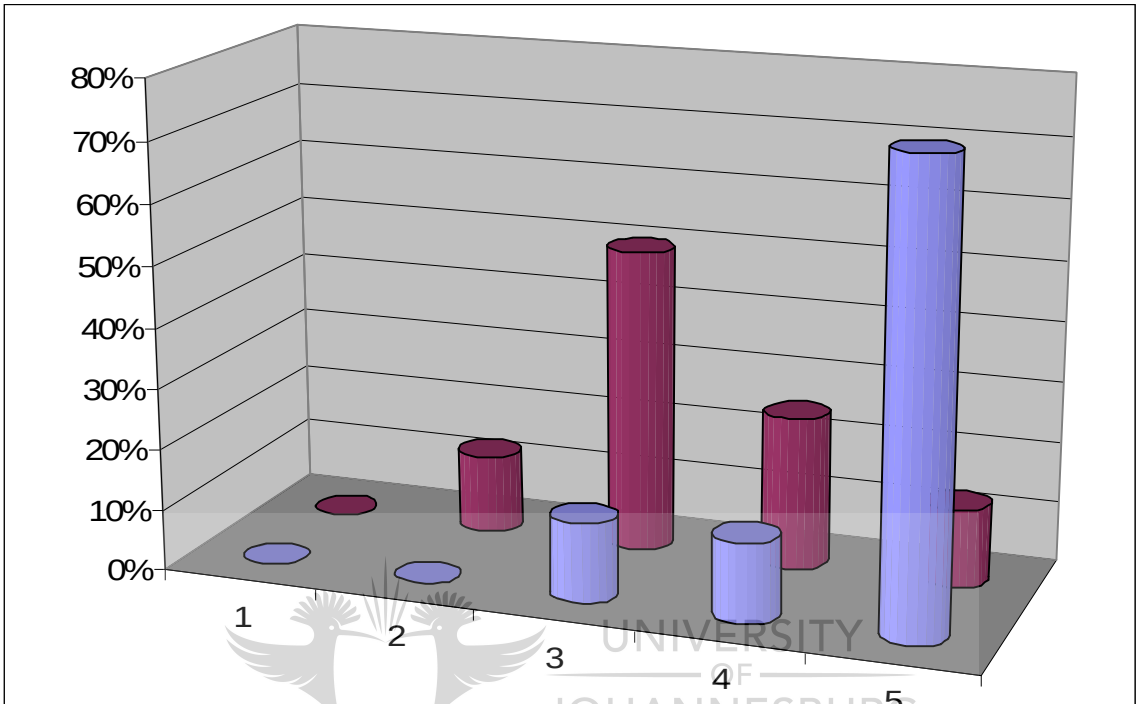





Considering the secure electronic storage of question papers, results of the importance against situation comparison (see graph 3.15) show that 75% of institutions recognise the importance of having a very secure PC or server to safeguard question papers electronically before they are written. However, 50% of the institutions perceive their current situation as being only average and 13% believe that the electronic safeguarding of question papers is poor.

This aspect of examination security needs to be critically controlled and guided by the IT or IS department, because many of the policy makers in the examination domain, if one considers their age and experience, may not be fully aware of the technical vulnerabilities associated with storing question papers electronically.

Graph 3.15 Is a very secure PC or server needed to safeguard the examination papers electronically before they are reproduced?




| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Importance | 0% | 0% | 13% | 13% | 75% |
| Situation | 0% | 13% | 50% | 25% | 13% |

Importance (at an ideal institution) 1 = not important, 2 = less important, 3 = average importance, 4 = very important, 5 = extremely important.

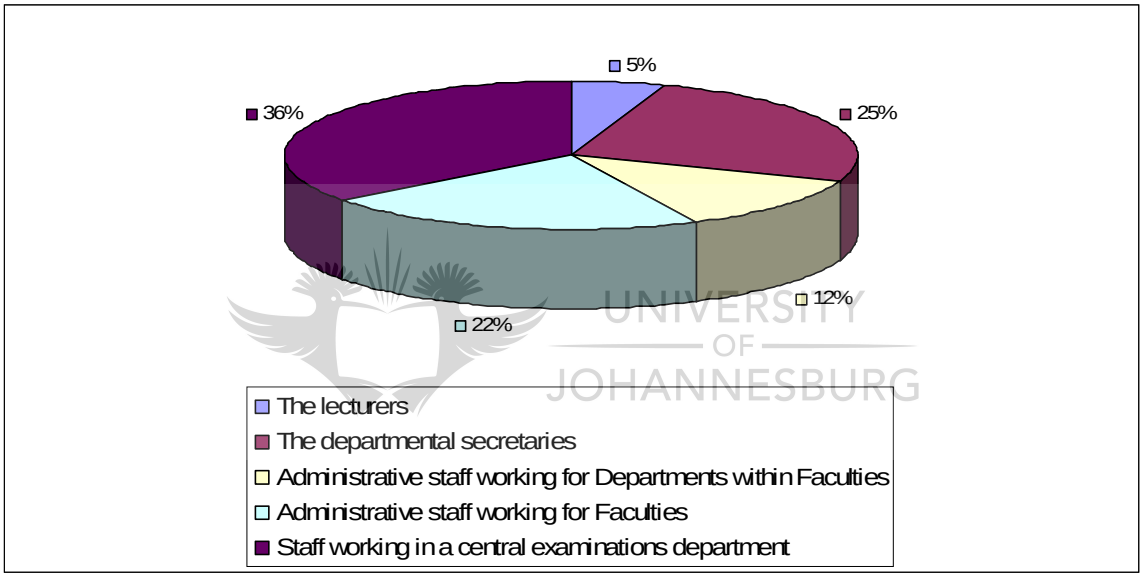
Situation (at all the institutions) 1 = very poor, 2 = poor, 3 = average, 4 = good, 5= excellent.

## 3.6 Finalisation of marks

Examination marks are regarded as the finalisation of the examination life cycle when it comes to the internal examination process of preparing for examinations, conducting examinations and then the capturing and publication of results.

When looking at the responses from institutions relating to who captures the examination marks, there was a mixed indication of where the responsibility resides. Most institutions (35%) indicated that staff working in a central examinations department capture marks, while either faculty staff, secretaries or lecturers capture marks in the remaining institutions (see graph 3.16).

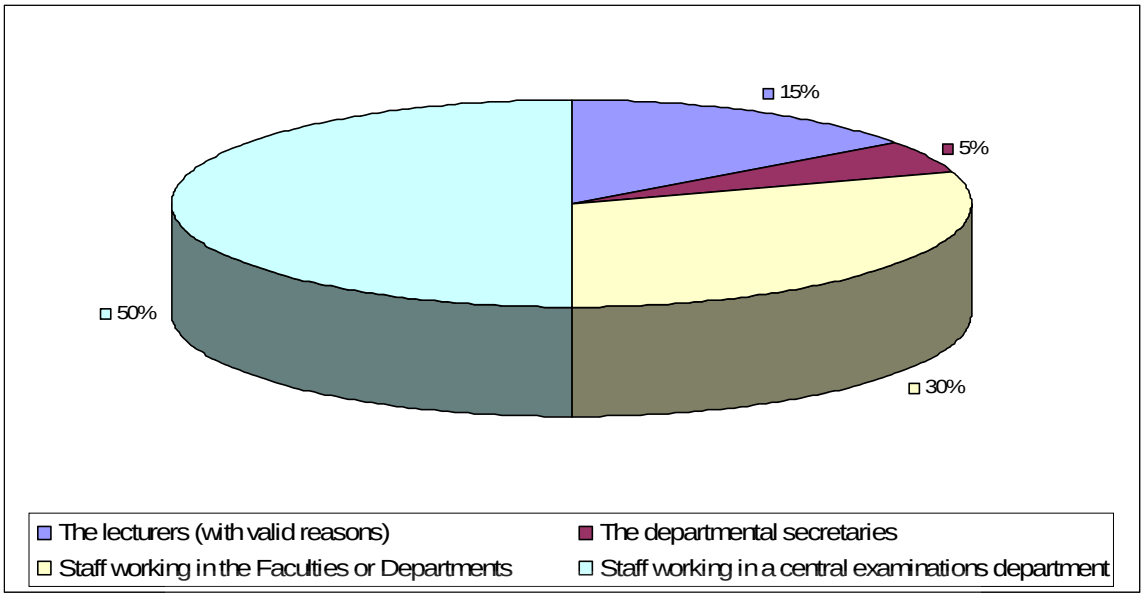
Graph 3.16 Who captures the examination marks?





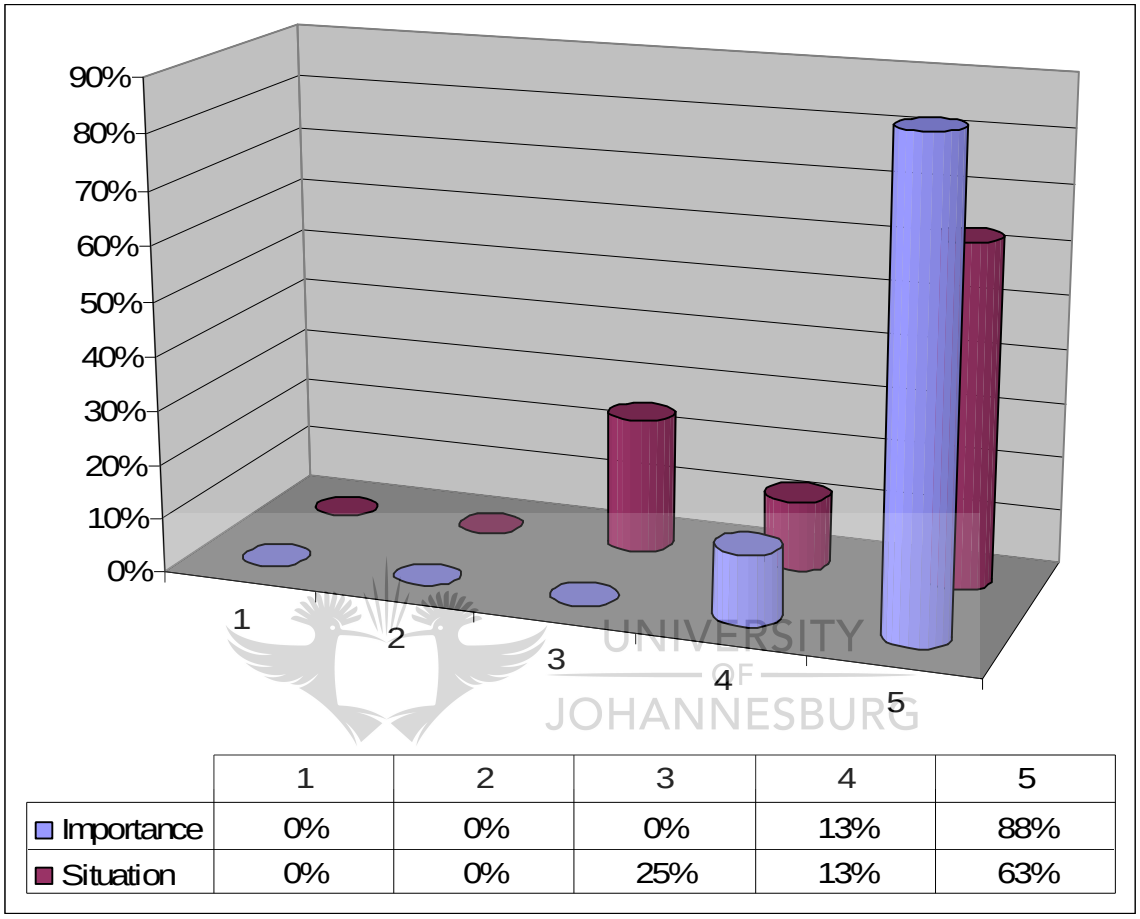

Further, it is necessary to consider who has the authority to amend marks after they have been captured on the institution's student system. In this case, there was also a mixed response, with 50% of the institutions responding that only staff working in the central examination department has the authority to amend marks. The rest of the respondents again reported that the faculty or lecturers are responsible for this function (see graph 3.17).

Graph 3.17 Who has the authority to amend marks?




The responses from all the institutions as reflected in the importance against the situation analysis indicated that 88% of institutions believe that it is extremely important to have a clear and understandable policy for the capturing and amendment of marks. Consistent with this finding, almost 80% of the institutions believe that their policies are either good or excellent (see graph 3.18).

Graph 3.18 Do you have a clear and understandable policy for the capturing and amendment of marks?



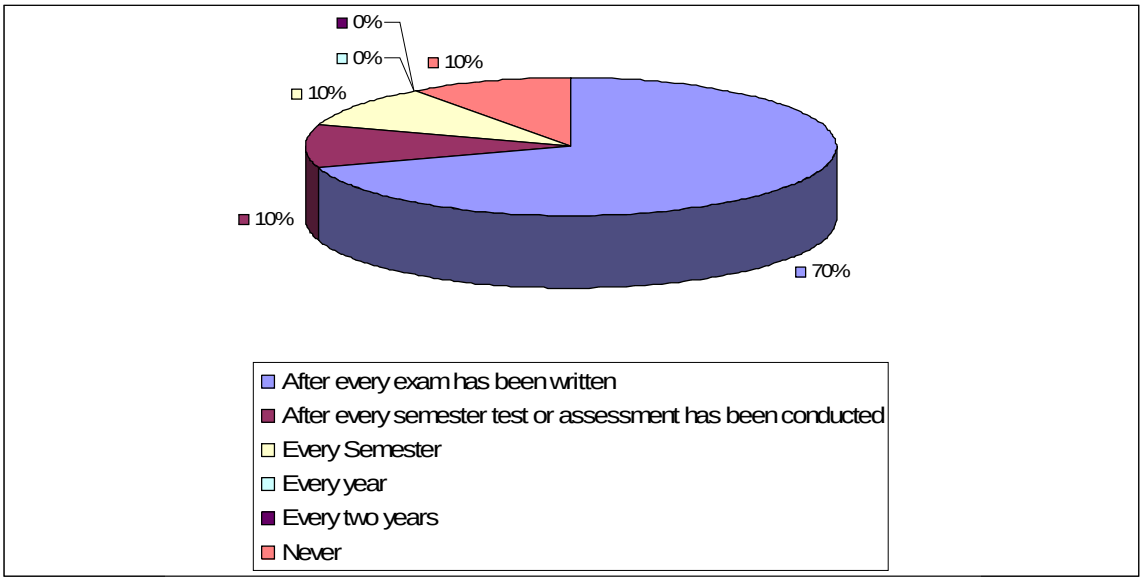

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Importance | 0% | 0% | 0% | 13% | 88% |
| Situation | 0% | 0% | 25% | 13% | 63% |

Importance (at an ideal institution) 1 = not important, 2 = less important, 3 = average importance, 4 = very important, 5 = extremely important.

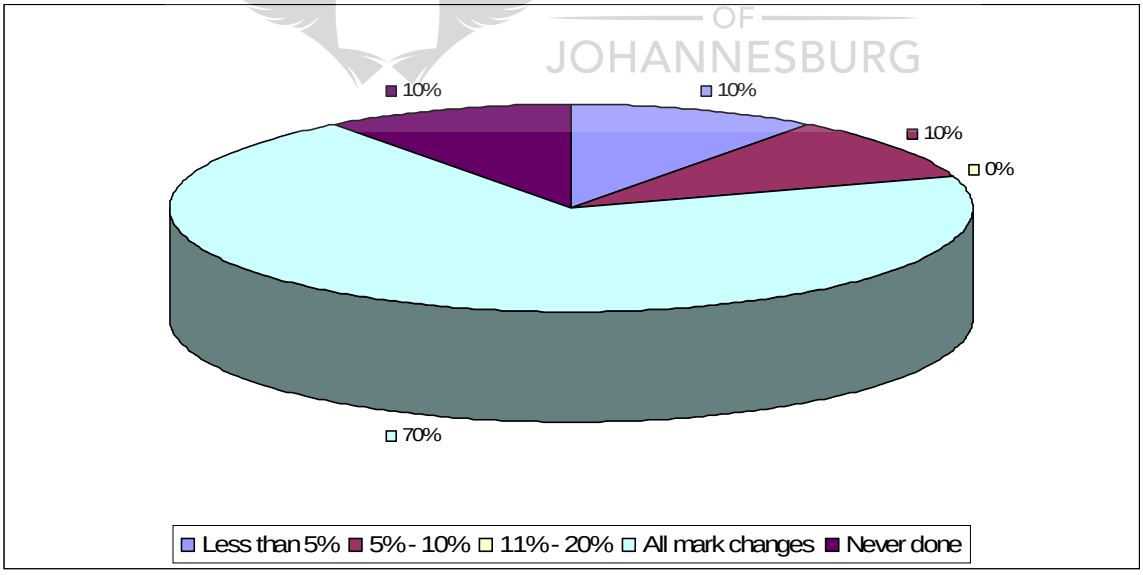
Situation (at all the institutions) 1 = very poor, 2 = poor, 3 = average, 4 = good, 5= excellent.

After the marks have been captured or amended by institutions mark audit, also come to the forefront. Ninety percent of institutions reported that they have a policy in place to regulate the capturing and amendment of marks. Further, 70% of the institutions reported that they audit marks after they have been captured and 70% audit all the mark changes (see graphs 3.19 and 3.20).

Graph 3.19 When are audits of mark changes done?




Graph 3.20 Audits of mark changes are done for marks that change by?

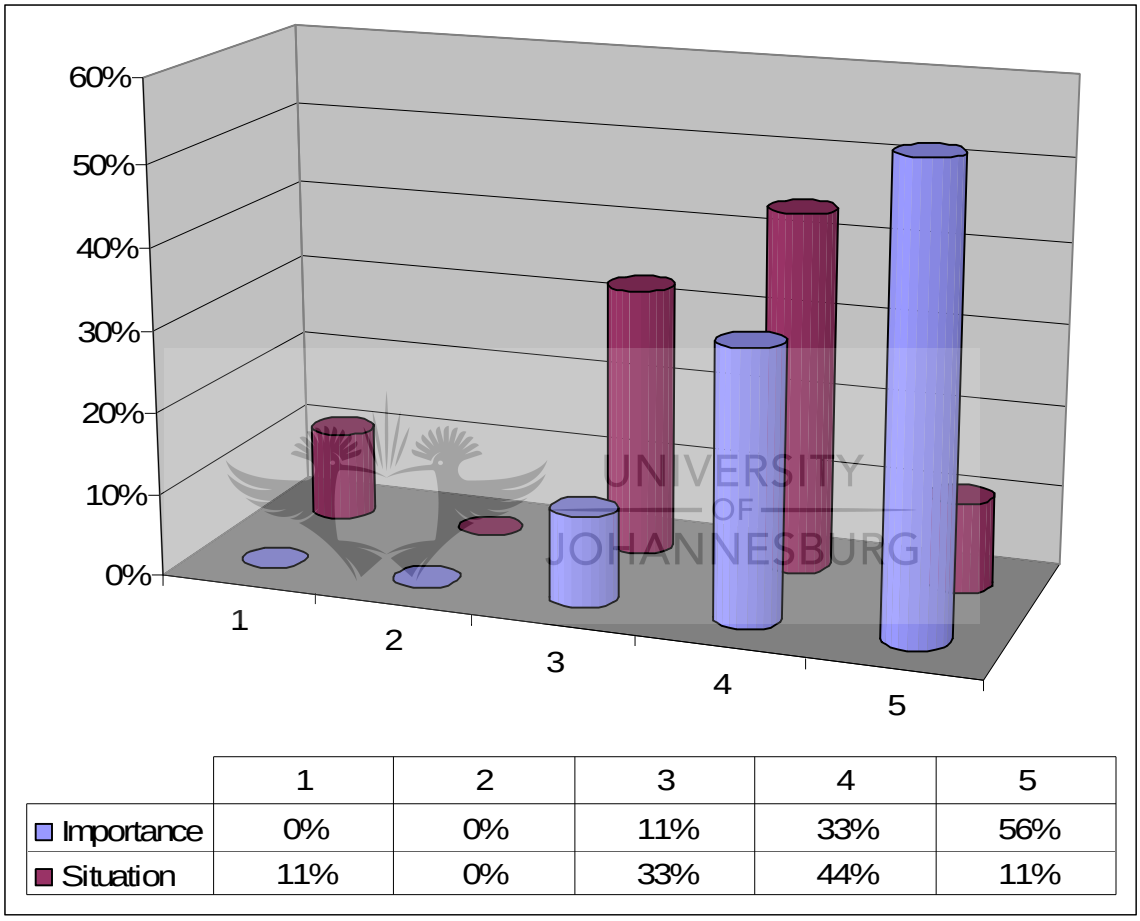





The responses from all the institutions reflect that only 56% of them believe that it is extremely important that mark amendment audits be conducted frequently.

The importance versus situation analysis is again consistent with this since 55% of institutions believed that their auditing of marks was above average (see graph 3.21).

Graph 3.21 Are mark amendment audits conducted frequently?




| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Importance | 0% | 0% | 11% | 33% | 56% |
| Situation | 11% | 0% | 33% | 44% | 11% |

Importance (at an ideal institution) 1 = not important, 2 = less important, 3 = average importance, 4 = very important, 5 = extremely important.

Situation (at all the institutions) 1 = very poor, 2 = poor, 3 = average, 4 = good, 5= excellent.

## 3.7 Closure

Risk factors within the examinations domain pose a real threat when it comes to the operational stability of any higher education institution. In today's competitive environment, technology needs to be utilised to not only survive, but also to compete for market share.

Global competitiveness is no longer only a weakness, but also a real threat when it comes to the market share retained by South African educational service providers. International educational institutions compete against South African institutions with an added advantage because of their willingness to embrace information systems in order to enhance and to expedite their administrative duties and thus gain a competitive edge by utilising secure electronic business processes.



Both the South African education environment and international higher education institutions are driven by the same fundamental goals. In the heat of operational pressures, institutions may lose sight of the fact that we are all part of the same continuum of skills and human resource development, with the added advantage of utilising technology to enhance administrative and examination processes.

# Chapter 4
# The use of information systems for improved examination processes and procedures

## 4.1 Introduction

The use of information technology has changed the way in which people do business and, particularly within the examinations environment, has encouraged the improvement of internal policy and procedures in order to strategically enhance and accelerate service delivery. Luftman (2004:35) notes that the concept of strategic alignment stresses the harmonisation of the goals and implementation plans of the IT department with the goals and organizational structure of the business as a whole. Today's IT executives have to concern themselves not only with technology, but they must also understand the strategic goals of the business in a dynamic and uncertain environment.



Providing an IT solution no longer involves just deciding on and implementing a software package for a department. There are specific organizational controls and processes that need to be taken into consideration. For example, departments that works with sensitive data that is critical in the business (e.g. examinations) need to consider security controls and password policies. This requires understanding and extra insight into the operational requirements of a department or organisation. In the examinations domain, which incorporates a spectrum of technologies in the process of planning, conducting and finalising examinations, it is vital to secure information and digital processes.

This chapter aims to explore the use of information systems that transform tertiary institutions into digital firms and the associated operational threats to the management of examinations in tertiary institutions in South Africa.

## 4.2 System security and access

Luftman (2004:166) notes that the majority of businesses do not have a companywide security policy, yet all companies that have an intranet, local area network (LAN) or a web site are subject to a number of potential security threats. Some of the better known security problems include unauthorised access to confidential data, illegal use or monitoring of e-mail systems and virus attacks. Thus, there is a need to create a controlled environment in which examination processes can be electronically enabled while maintaining the highest level of security and controls.



A positive finding of the current study is that 100% of the respondents stated that the PCs used in the examinations department are password protected. However, it is concerning to note that 20% of respondents stated that these passwords are never changed. The study found that all the institutions surveyed believed that, at an ideal institution, it would be extremely important that local PC and network passwords be updated frequently. However, when rating themselves in terms of this aspect, 67% of institutions rated themselves as average and 33% classed themselves as being above average. This provides some insight into the institutions' internal controls, and suggests that many institutions feel that they need to strengthen their security relating to password protection and the overall controls of using electronic media for examination operations.

According to Luftman (2004:334) there must be a mutual understanding between the business and IT functions in order to achieve the goals of the organisation which such mutual understanding derives from both the business function understanding the world of IT and the IT function understanding the business world. This principle of sharing and understanding the critical needs and threats within the organizational structure needs to be stressed. In the examinations environment, is the implementation ad enforcement of security. The examinations department would not understand the threats associated with the access granted to every PC by the administrator password if information about this critical function was not provided by the IT department.

PCs are set up with the software necessary for use as a business tool in an organisation and an administrator account and a user account is created. Fifty percent of the respondents stated that their IT department keeps this administrator account password. The question that thus arises is whether the IT department understands the security threat associated with this account if the password is not securely administered or safely guarded. Access to the administrator account password effectively allows data on the PC to be spied upon, copied or amended without the user knowing this has been done. The research found that 63% of respondents believe that the IT department should not have access to the administrator password for PCs used in the examination domain but only 13% of institutions thought that their current situation is either good or adequate in terms of the administrator account password.



It is necessary to interrogate whether the IT or IS department needs to have the administrator passwords for the PCs of examination staff and whether examination managers know the security risk that this poses and that there should be controls in place to manage this. Controls, according to Laudon and

Laudon (2002:441), consist of all the methods, policies, and organizational procedures that ensure the safety of the organization's assets, the accuracy and reliability of its accounting records, and operational adherence to management standards. In contrast to the enforcement of such controls, the administrator account password allows personnel from outside the examinations department to have full access to all examinations data. This means that if the security of the administrator password was compromised or even if IT staff misused it, they could monitor all work done by examination staff on their PCs. Thus if examination staff are typing examination papers or capturing marks, unauthorised people who are outside the secure domain of examinations could intercept, sabotage or change critical data without the knowledge of the institution or the examination manager.



According to Whitman and Mattord (2003:42) in order to make sound decisions about information security and to create policies and enforce them, management must be informed about the various kinds of threats facing the organisation. The organisation's IT Department must therefore, take responsibility for informing and warning the organization about potential threats. This is particularly important in critical departments like examinations, which increasingly use technology to enable them to provide online learning and assessments.

Today the internet is the preferred medium of communication between an institution and students because of its ease of use, speed in disseminating information and the ability to obtain information anywhere in the world. The benefits of using the internet, according to Laudon and Laudon (2002:280-281), include its global connectivity, ease of use, low cost and the ability to create interactive multimedia capabilities. By using internet technology, organizations

can reduce communication and transaction costs, enhance coordination and collaboration and accelerate the distribution of knowledge.

When one considers business processes within the examinations domain, information technology has advanced significantly with the use of web technology to enhance communication between students (clients) and the institution. The policy makers or examination managers thus need to embrace and manage the use of new technology to gain advantage but still maintain adequate system security . In order to determine acceptance of and willingness to use technology this study included certain demographic parameters such as the age, experience and the educational level of policy makers in order to model the average examination manager in higher education in South Africa.

Seventy percent of the policy makers were aged between 51 to 60 years old and 50% of them have at least 10 years experience in the examinations domain. The remaining 50% have at least 5 to 10 years experience. Another indicator that was used was the educational level. Fifty percent of respondents have degrees, 20% have a diploma and 10% have obtained a Doctorate. Thus, the kind of person who is in charge of the examinations at institutions in South Africa tends to be educated, experienced and relatively senior in terms of age. An interesting result was the gender profile with 40% of managers being female, which reflects gender equity in the examination domain.

## 4.3 E-mailing and the preparation of examination documents

Today, e-mails are widely accepted as the preferred medium of business communication because of the speed of delivery and worldwide availability.

Laudon and Laudon (2002:186) describe e-mail as a tool, which is used for the computer-to-computer exchange of messages, and note that it is an important medium for communication and collaborative work. E-mail technology is being utilised to expedite service delivery in the examination domain by enhancing services in areas such as examination queries from students and academics and general business communication.

In order to fully utilise this medium, 85% of institutions believed that it is extremely necessary to password protect examination papers when they are sent via e-mail to the examinations department. However, almost 30% of institutions rated themselves as being below average as this control was not adequately or effectively enforced. The heightened vulnerability of data that is sent electronically has created special concerns for the policy makers who manage examination processes. While electronic business operations do enhance business processes they need to be extra secure and extra stable when managing examinations.



Critical care also needs to be exercised when preparing question papers. Even if there is a policy that controls security from the point of submitting examination documentation to the examinations department, there is always vulnerability outside the examinations department. This study established that departmental secretaries or assistants type examination papers in 80% of institutions in South Africa. Thus, even if the examinations manager enforces policies, procedures and controls all the electronic media associated with examinations, in the examinations department human factors also need to be considered. There is always the possibility that staff may be corrupt and may sell examination papers they have typed or change marks that have been submitted.

Luftman (2004:166) states that security planning and management starts with a review of those operational areas that have the greatest financial impact on the firm. Organisations need to evaluate what would happen if the system application, web site or database were disabled, damaged, hacked or destroyed and ascertain whether the business could survive that kind of loss. In the examination domain, data integrity and security is of the utmost importance if the institution is to remain a reputable provider of education in South Africa. Policy makers need to ask themselves how important security planning and the management of security are for them. They need to be thoroughly familiar with security management so that they are aware of the vulnerabilities in the domain. In addition, they should know how to effectively manage the security of ongoing re-definition and deployment of technology products in their environment (e.g. the use of e-mail as a primary communication tool for examinations).



## 4.4 Safeguarding of examination papers

Laudon and Laudon (2002:438) define security as the policies, procedures, and technical measures used to prevent unauthorised access, alteration, theft or physical damage to information systems. Nowhere is security more important than in the examinations domain in order to ensure that the reputation of the institution is not damaged. It is much easier to safeguard a printed examination paper than an electronic one because the examinations department can just lock it up inside a strong room or safe and physically control security access to the safe. In contrast, safeguarding electronic examination papers on a PC or server requires technical measures and security policies in order to prevent unauthorised access. This security requirement needs significant operational insight into the examination department's security needs by the IT or IS department.

Considering the safeguarding of electronic examination papers before they are written, 75% of institutions asserted that it is extremely important to have a very secure PC or server to safeguard question papers electronically before they are written. However, 50% of institutions stated that their safeguards were only average while 13% reported them as being poor. The IT or IS department has a vital role to play in this aspect of examination security, because if one considers the age and experience of many of the policy makers in the examination domain, many may not know about the technical vulnerabilities associated with the electronic storage of question papers.

## 4.5 Online submission and control of marks



According to Laudon and Laudon (2002:441) special policies and procedures must be incorporated into the design and implementation of information systems in order to minimize errors, disaster, interruptions of service, computer crime and breaches of security. The combination of manual and automated measures that safeguard information systems and ensure that they perform according to management standards, is termed controls. Controls in the examinations domain thus needs to be defined to guide the management of marks as one of the primary electronic environments of ensuring security in the examinations domain.

From a control point of view, 88% of institutions reported that they have a clear and understandable policy on the capturing and amendment of marks. Similarly, the situation analysis reflected that 76% of the institutions indicated that the capturing and amendment of marks was either good or excellent.

Another form of control is the continuous auditing of marks that have been changed on the system. Ninety percent of the respondents indicated that they conduct mark audits. At 70% of the institutions, these audits are done for all mark changes on the system. Eighty nine percent of institutions deemed mark audits to be of above average importance. Moreover, the situation at these institutions reflected that only 55% of them were enforcing mark audits actively.

In the examinations domain, electronic business processes also allows the use of SMS technology to facilitate the dissemination of examination information to a broader spectrum of technology users. SMS technology can now be integrated with the institution's communication strategy in order to communicate more effectively, faster and on a more personal note with students or staff and can be used for example to notify students of their marks.



## 4.6 Information Technology or Information Systems support

Whitman and Mattord (2003:41) state that both general management and IT management are responsible for implementing the information security that protects the ability of the organisation to function. Although many business and government managers shy away from addressing information security because of its perceived technical complexity, it is important to understand that information security has more to do with management than with technology.

Many managers in the examinations department consider their responsibility for security to lie only in the physical and paper domain. Although they understand that protecting their business processes when using electronic resources requires significant understanding and input from their department, they still rely greatly on their Information Technology department and have minimum input to

or understanding of this process. In this study, institutions reported that 75% thought that it is extremely important that the Information Technology department be involved in reporting and guiding them through technological vulnerabilities in the examination environment. However, only 63% of the institutions regarded the IT departments' involvement as average and 13% believed that it was very poor.

The above discussion provides a good indication of how well institutions are managing their examination department's technological vulnerabilities in consultation with their Information Technology or Information Systems department's skills and expertise.

## 4.7 Closure



Global competitiveness is a real threat when it comes to the market share retained by South African educational service providers. International institutions are competing against South African institutions on a more advanced level because of their willingness to embrace information systems to enhance and expedite their administrative duties.

A balance needs to be found between utilising advances in technology, for instance e-mail and the internet, to enhance communication and administration in the examination department without compromising security and quality. Thus focusing on examination security processes that neither over controlled nor under controlled with the added advantage of adequately addressing operational requirements within the examinations department.

Information technology has influenced most on the business processes within the examinations domain. The use of web technology, e-mails and telephone system

technology has enhanced communication between students (clients) and institutions greatly.

# Chapter 5
# Operational strategies to manage the security needs within the examinations domain

## 5.1 Introduction

Chen (2001:103) argues the fact that a key benefit that electronic business offers is the ability to accelerate all the processes involved in the business: buying, selling, manufacturing and distribution. In the case of educational service providers this would translate into marketing, registering students, student administration and graduating a student. For this to be effective, the bulk of the electronic administration (which is student administration) needs to be efficient and beneficial to the institution.



Policies and procedures in the examination domain thus need to be fully integrated with the electronic business processes of the department in order to guide and expedite the administration of examinations. It is no longer possible for examination staff to independently conform to or amend procedures relating to administration in their environment. It is now essential to involve information technology staff in order to allow them to guide decisions about technological vulnerabilities and security threats.

This chapter explores use of information systems in tertiary institutions and the associated operational threats tertiary institutions in South Africa face in the management of examinations.

## 5.2 System security and access

Whitman and Mattord (2003:64) explain that an attack is a deliberate act that exploits vulnerability. An attack is carried out by means of a threat agent that damages or steals an organisation's information or physical asset. What does this mean? According to Whitman and Mattord (2003:64), an exploit is a technique that compromises a system. Vulnerability is an identified weakness in a controlled system in which controls are either not present or are no longer effective. An attack is the use of an exploit to compromise a controlled system. The first and foremost strategy for an examinations manager should thus be the identification of technical weaknesses in operational procedures in the examinations domain.



Whitman and Mattord (2003:42) stress the fact that management should be informed about the various kinds of threats facing the organisation by the information technology department. The information technology department must, therefore, take responsibility for informing, warning and guiding high-risk organisational departments such as examinations.

Only when the examination manager is aware of the weaknesses would he/she be able to address the vulnerabilities within the examinations department. The principle of sharing and understanding critical needs within the organisational structure needs to be emphasised. Luftman (2004:334) argues that there should be a mutual understanding between different departments in order to strengthen the partnership between the departments in order to achieve the goals of the organisation. This means the examinations function must have an understanding

of the world of the information technology Department and the information technology function must understand the needs and constraints of the examinations department.

This study established that 20% of staff in the examinations domain never change their PC passwords, which should be the first area of concern for the IT department and examinations manager. Passwords and the policy that regulates them should be a vital consideration in an institution, particularly in the examinations domain. Examination managers must understand that this is a real threat to the examinations environment and that the manager is responsible for managing this threat. Only with the expertise, help and guidance of the IT department can this vulnerability be managed by, for example, configuring the systems to automatically ask for a new password regularly and by managing the staff and sensitizing them to the threat by implementing a password and access policy.



Luftman (2004:213) questions whether organizations should be more concerned about security threats from outside or inside the organisation. Research suggests that the greatest threat may be from those “inside the walls”. Consistent with such research, this study fount that 50% of institutions allow their IT department to keep the administrator accounts for the PCs in the examinations department, although 63% of the institutions said that they do not think that it is necessary for the IT department to have full control over their PCs. This may pose a significant threat to the examination domain because, as research suggests the greatest threat may be from staff working for the institution.

According to the survey, most of the examination managers do not seem to be fully aware of the potential risks posed by the administrator account. Also of

concern is the fact that their Information technology departments have not yet explained the necessity of retaining the account nor the security measures that have been put in place to regulate it.

Examination managers must be made aware of this potential security risk and manage it in the same way as any other physical or technological risk is managed. It is the Examination manager's responsibility to take exert control over this situation and either compel the information technology department to give responsibility for the administrator passwords to the examinations department or, alternatively include them in the security management of the department. Inclusion in the security management of the department means that the IT department is subject to all the rules and regulations applicable to staff working directly for the department, for example policy on the regular changing of passwords and the signing of a confidentiality document to safeguard confidential information and intellectual property.



## 5.3 E-mailing and the preparation of examination documents

Most of the institutions (85%) stated that it is extremely important to password protect examination papers before they are e-mailed, but only 30% said that this is currently done in their institution. This would constitute a significant risk for the examinations department if they decide, for operational reasons, that staff should only submit examination papers electronically via e-mail, but the necessary security requirements to effectively and securely manage electronic submissions are not in place.

Whitman and Mattord (2003:64) define information security as the protection of information and the systems that use, store or transmit such information from

danger by the application of policy, education and technology. The use of passwords to protect examination papers must thus be seen as a critical element in the protection of information and should again be enforced through the application of policies, procedures and regulations. The use of this electronic medium (e-mail) must, therefore, be fully documented in the policies and procedures of both the examination department and the information technology department. The security regulations governing the password protection of examination papers before acceptance by the examinations department should be explained.

Such formalisation of policies and procedures concerning the security requirements for electronic media will ultimately compel the examination department an information technology department to engage with each other to assist with the definition of duties and clarification of roles and responsibilities. This will also ultimately result in the official documentation of the critical issues that have highlighted in this document.



## 5.4 Safeguarding of examination papers

Whitman and Mattord (2003:55) postulate that evidence of a crime is not readily apparent when electronic information is stolen. If thieves are clever and cover their tracks carefully, no one may ever know about the crime until it is far too late. Thus the safeguarding of electronic examination papers, particularly the prevention of electronic theft, must be one of the most important security concerns for an examination manager. Obviously, the examination manager would not be required to have the technical skills required to enforce electronic security within the department, but the guidance and assistance of the information technology department would be needed. The security of electronic

business throughout the industry must ultimately be the responsibility of the information technology department because they are tasked and equipped with the resources and skills to manage it. It must, therefore, be clearly stipulated that their input and skills are a major cornerstone of the security infrastructure of any examinations department.

Seventy five percent of institutions surveyed stated information technology assistance is extremely important, but 13% reported that the current level of support received is very poor. Such lack of assistance needs to be brought to the attention of management and should be clearly identified this as a key risk area in the security requirement of any examinations department. The information technology department must be tasked with the responsibility of ensuring security continuity because the necessary technical skills do not reside with the examinations domain. Thereafter the security policy of the examinations department must include the responsibilities of all parties involved and the security regulations to ultimately ensure security of examination papers that are electronically stored.



## 5.5 Online submission and control of marks

According to this research formal policies and procedures to regulate the control of marks do seem to be adequately managed. There also seem to be strict audit measures in place to regulate the amendment of marks. This is probably the result of the formal educational quality controls put in place by the Department of Education to regulate quality at tertiary institutions in South Africa.

Many of the existing requirements stipulated by the Department of Education and formal audit practices include the formal audit and control by means of policies

regulating the submission and amendment of marks. This process should be closely scrutinised from a technological point of view since electronic business processes have started to intertwine with existing policies and procedures. For example, whereas marks historically have been submitted on printed classlists, academics now are able to import their marks into the system or even capture them online on a website or intranet. Consequently, examination managers should ask their information technology department whether there are any security risks that need to be managed.

## 5.6 Information Technology or Information Systems support

Whitman and Mattord (2003:72) state that an organization's senior management is accountable for information security. The Information technology department may also have security responsibilitiesl. An organisation needs information security for four important reasons: to protect the ability of the organisation to function; to enable the safe operation of applications; to protect the data an organisation collects; and to safeguard the technology assets in a organisation by adding secure infrastructure services based on the size and scope of the enterprise. The responsibility thus lies with the information technology department to adequately inform examination managers about the security requirements of every aspect of electronic business processes incorporated into their operational business processes.



This survey concluded that 75 % of institutions think that it is extremely important that their information technology department guide them when introducing a new electronic business process into their environment. However, 63% of institutions considered the support given as being only average and 13% reported that the guidance is poor. The support and responsibility should lie with the department

which has the skills and expertise to support the information security function such as enforcing network passwords or keeping the administrator passwords. The information technology department must disclose the risks and threats to the examination manager and document the responsibilities accordingly.

Whitman and Mattord (2003:64) explain that upper management drives the top down approach to security implementation. Thus while the IT department shold provide support and guidance examination managers should take responsibility for managing their security issues. Such security issues include not only the physical or operational examination issues, but also electronic business process issues. This study found that examination managers are not adequately involved in the management of electronic security requirements in their departments.

Policy and procedural documents must include the electronic media utilised by the business such as the use of e-mail technology to submit examination papers. For audit purposes, they should include the potential risks and mitigating actions implemented such as password protecting documents before they will be accepted via e-mail. It is clear that the required technical support from the information technology department for examination management is lacking.



## 5.7 Closure

Luftman (2004:213) explains that the 21st century brings with it an astonishing array of information technology that is distinguishing this period from previous ones. The success of the internet, wireless computing and dozens of other new technologies raises questions, such as: how does an organisation effectively

manage the technology? How will the organisation be affected by the technology? How does the technology drive organizational change and design?

Advances in technology should be seen as an opportunity, especially in the case of managing examinations at tertiary education institutions in South Africa, to expedite service delivery and enhance business processes. However, the assistance of the information technology department is necessary to control and manage the electronic business processes adequately.

# Chapter 6
# Conclusion and Recommendations

## 6.1 Conclusion

The critical challenge for institutional leaders today is how to manage security amidst the phenomenal advances is technology. Underpinning this challenge is the necessity for institutions to adapt and implement new technologies in order to advance technologically and to remain competitive.

Many managers in the examinations domain consider their responsibility for security to lie only in the physical and paper domain in the examinations department. Although they understand that protecting their business processes when using electronic resources will require significant understanding and input from their department, they still rely greatly on their information technology department that has minimum input into or understanding of the examination department's process. In this study, 75% of the respondents thought that it is very important that the information technology department be involved in reporting and assisting with vulnerabilities that exist in an examination environment that uses technology. However, in contrast, 63% of institutions that took part in the study reported that they currently receive only average support from the information technology department while 13% reported that the input they receive is poor.

This survey concluded that 75% of institutions that took part in the study believe that it is extremely important that their information technology department guide

them when introducing new electronic business process into the examination environment. However 63% of them reported that such guidance is only average while 13% reported their situation to be poor. Support of and responsibility for electronic business processes should lie with the department which has the skills and expertise to support the function. Such expertise would include enforcing network passwords or keeping the administrator passwords. The information technology department should disclose the relevant risks and threats to the examination manager and document the responsibilities accordingly.

The use of information technology in the examination department of educational institutions requires a new security culture and infrastructure that allow institutions both to support secure business processes as well as to provide stable electronic educational services.



According to the survey, most examination managers are not fully aware of the potential risks the administrator account exposes them to. More concerning is the fact that their Information technology departments have not yet informed examination managers about why they keep the administrator passwords nor have they explained what security measures they have put in place to regulate the passwords. Examination managers must be made aware of this potential security risk and manage it in the same way as any physical or technological risks are managed.

It is the Examination manager's responsibility to take control of this situation and either ensures that the information technology department hands over responsibility for the administrator passwords to the examinations department. Alternatively, the information technology department should be included in the security management of the department. Such management of security should

include all the rules and regulations that are applicable to staff working directly for the department, for example the policy for the changing passwords regularly and the signing of a confidentiality document to safeguard confidential information and intellectual property.

Such formalisation of policies and procedures to include the security requirements of electronic media will ultimately compel engagement with the information technology department in order to assist with the definition of duties and the clarification of roles and responsibilities. This will also ultimately result in the documentation of critical issues that have highlighted in this research.

Policy and procedural documents must address the electronic media of business such as the use of e-mail technology to submit examination papers. They should include the risks and mitigating actions taken for audit purposes, for example password protecting documents before they will be accepted via e-mail. It is clear that, presently, the required technical support for examination management from the information technology department is lacking.



There is a lack of a proper strategy to manage examination security at South African tertiary educational service providers, particularly when it comes to the implementation and use of information technology to drive secure electronic business processes.

There is a simple conclusion to be drawn from the concerns highlighted by this research: Electronic policies and procedures seeking to raise the quality of examination administration must provide more help and less insecurity.

## 6.2 Recommendations

Information technology departments at tertiary institutions in South Africa do not adequately support the needs of examination managers concerning the security requirements of electronic business processes. Examination managers rely fully on the skills and expertise of the information technology department to guide, inform and warn them about the use of electronic business processes within the department. Their involvement needs to be secured and prioritized by top management.

Formal policy and procedural documentation should incorporate both the existing use of electronic media (such as e-mailing examination papers) and their associated electronic security controls. This conforms with operational audit requirements and sound business practices relating to electronic data security within every institution.



Policies and procedures in the examination domain thus need to be fully integrated with the electronic business processes of the information technology department in order to guide and expedite the administration of examinations effectively. Examination staff can no longer independently conform or amend procedures relating to administration in their environment. The involvement of their information technology staff is necessary to guide decisions about technological vulnerabilities and security threats.

The information technology department's use of the administrator password on computers used for examinations is a critical security risk, and must be

communicated, documented and formally managed by the examination manager who must, ultimately, accept responsibility for his/her domain.

Advances in technology should be seen as an opportunity, especially in the case of managing examinations at tertiary education institutions in South Africa, to expedite service delivery and enhance business processes. However, it is essential to control and manage the electronic business process adequately with the assistance of the information technology department.

# LIST OF REFERENCES

Berge ZL. 1996. *Obstacles to distance training and education in corporate organizations*: Journal of workplace learning, 14(5):182-189.

Chen S. 2001. *Strategic Management of e-Business*: John Wiley & Sons.

Cooper DR & Schindler PS. 1998. *Business research methods*: McGrawHill.

Dillon WR, Madden NHF & Firtle NH. 1993. *Essentials of Marketing Research*: Von Hoffman Press.

Laudon KC & Laudon JP. 2002. *Management Information Systems (Managing the digital firm).* 7th Edition. Prentice Hall.

Le Roux M. 2005. *Mbeki praises role of universities in South Africa.* Mail and Guardian, 15 March 2005:4-5.

Luftman JN. 2004. *Managing the Information Technology resource (leadership in the information age)*: Pearson.

Mouton J. 2002. *How to succeed in your Masters and Doctoral Studies: South African Guide to Research:* Van Schaik.

Norris G. 2000. *Business and ERP (Transforming the Enterprise).* 1st edition. Price Waterhouse Coopers.

Roberts P & Chambers M. 2001. *Digital Developments in Higher education: Theory and Practice:* Cambridge.

Shelly GB, Cashman J & Vermaat ME. 2005. *Discovering Computers 2006: a gateway to information:* Thomson course technology.

Stacey RD. 1993. *Strategic Management and Organizational Dynamics: The challenge of Complexity* .1st Edition. Prentice Hall.

Whitman ME & Mattord H. 2003. *Principles of information security:* Thomson course technology.

Zlikmund WG. 2003. *Business research methods.* 7th Edition. Thompson Learning.

## EXAM SECURITY QUESTIONNAIRE

The following questionnaire has been prepared to evaluate the use of technology for managing exam security at Tertiary Institutions in South Africa. We would appreciate your assistance in this research, which is part of a MBA dissertation.

Please answer the following questions as honestly as possible. **All answers will be treated in the strictest confidence.** It will take no longer than 15 minutes to complete the questionnaire.

**Should you have any queries, please do not hesitate to contact the researcher – Mr. Tinus van Zyl (082 560 6861 or 011 406 8045)**

There are 3 sections to this questionnaire. Please complete all 3 sections.

### SECTION A

In this section I would like to gather some operational informational to determine the technology needs and use at your Institution. Indicate your answer by means of a cross (X) in the appropriate block (Please indicate also if more that one answer is applicable).

1 Are you working at a

| | |
|---|---|
| University | |
| Technikon | |
| Recently (in the last 2 years) merged Institution | |
| Other- | |



2 Your age in years

| | |
|---|---|
| 20 or younger | |
| 21 – 30 | |
| 31 – 40 | |
| 41 – 50 | |
| 51 – 60 | |
| 61 – 70 | |
| 71 and above | |

3 Your gender

| | |
|---|---|
| Male | |
| Female | |

4 Highest educational level achieved

| | |
|---|---|
| Some secondary school | |
| Grade 12 / Matric | |
| Diploma | |
| Degree | |
| Masters degree | |
| Other qualification- | |

5 How long have you been involved at your Institution with the administration of examinations?

| | |
|---|---|
| Less than 1 year | |
| At least 1 but less than 2 years | |
| At least 2 but less than 5 years | |
| At least 5 but less than 10 years | |
| At least 10 years | |

6 The administration of exam related duties are done?

| | |
|---|---|
| Centrally (central exams department for the whole institution) | |
| Decentralised to faculties (every faculty manages their own exams) | |
| Decentralised to the departments reporting to faculties | |
| Other- | |

7 How many staff, students and exam papers are administered (indicate with appropriate number)?

| | Number of full time staff | Number of full and part time students | Average number of exam papers written every semester |
|---|---|---|---|
| Central exams Dept | | | |
| Decentralised to faculties | | | |
| Decentralised to the departments reporting to faculties | | | |
| Other- | | | |



8 How many students do you have presently at your Institution for this year?

| | |
|---|---|
| Less than 10 000 | |
| At least 10 000 but less than 20 000 | |
| At least 20 000 but less than 30 000 | |
| At least 30 000 but less than 40 000 | |
| More than 40 000<br>Specify: | |

9 Are the following people involved with the typing of examination question papers?

| | Yes | No |
|---|---|---|
| The lecturer who presents the class | | |
| With assistance from secretaries, but mostly by the lecturers who presents the class | | |
| Departmental secretaries or assistants | | |
| Typists or staff working in a central examinations department | | |
| Other – | | |

10 Where are exam papers reproduced, printed or photocopied before they are written?

| | Yes | No |
|---|---|---|
| At the lecturers office or department | | |
| At the departmental secretaries or administrative assistants office | | |
| At dedicated printing stations (for exam and test papers only) in the department or faculty | | |
| At typists or staff working in a central examinations department (in their office) | | |
| At a central printing station dedicated to printing examination papers for the whole of the Institution | | |
| Other – | | |

11 Who safeguards the exam papers before the examinations are written?

| | Yes | No |
|---|---|---|
| The lecturers | | |
| The departmental secretaries | | |
| Administrative staff working for Departments within Faculties | | |
| Administrative staff working for Faculties | | |
| Staff working in a central examinations department | | |
| Other – | | |

12 Who captures the exam marks on the Institution's student administration system?

| | Yes | No |
|---|---|---|
| The lecturers | | |
| The departmental secretaries | | |
| Administrative staff working for Departments within Faculties | | |
| Administrative staff working for Faculties | | |
| Staff working in a central examinations department | | |
| Other – | | |



13 Who has the authority to amend marks on the Institution's student administration system?

| | Yes | No |
|---|---|---|
| The lecturers (with valid reasons) | | |
| The departmental secretaries | | |
| Staff working in the Faculties or Departments | | |
| Staff working in a central examinations department | | |
| Other – | | |

14 When are audits of mark changes done?

| | |
|---|---|
| After every exam has been written | |
| After every semester test or assessment has been conducted | |
| Every Semester | |
| Every year | |
| Every two years | |
| Never | |
| Other – | |

15 Audits of mark changes are done for marks that change by:

| | |
|---|---|
| Less than 5% | |
| 5% - 10% | |
| 11% - 20% | |
| All mark changes | |
| Never done | |
| Other – | |

16 Are the PC's used to type exam papers and capture exam marks on, password protected?

| | |
|---|---|
| Yes | |
| No | |

17 How often are the passwords on these PCs changed?

| | |
|---|---|
| Every day | |
| Every week | |
| Every month | |
| Every year | |
| Never | |
| Other – | |

18 Every PC is set up with an administrator account and a user account which is used to log onto the machine. With the password to the administrator account of a PC one can get access to everything on it and copy, delete or even view what is happening on that machine remotely at any time. Who keeps the administrator passwords to the PC's used to type exam papers and to capture exam marks?

| | |
|---|---|
| Every person keeps his/her own PCs administrator password | |
| Central IT Department | |
| The Head of every Department | |
| Other – | |



19 Do you have a policy in place to regulate the capturing and amendment of marks on your student administration system?

| | |
|---|---|
| Yes | |
| No | |

**SECTION B**

In this section of the questionnaire, I would like to test your opinion of a few statements about the exam security of your institution in particular.

Firstly, you have to indicate in the FIRST COLUMN how important the item is in **your opinion at an ideal institution**. If you think a particular issue is EXTREMELY IMPORTANT, circle the 5 or if you think it is NOT IMPORTANT AT ALL, circle 1 or any other number that represents your opinion between 1 and 5.

In the SECOND COLUMN you have to indicate **the situation at your institution** with regard to each item. If you think your institution is EXCELLENT, circle the 5 or if you think your institution is VERY POOR circle 1 or any other number that represents your opinion between 1 and 5.

| **IMPORTANCE** At an ideal Institution | | | | | | **SITUATION** At your Institution | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| NOT IMPORTANT AT ALL | ⟷ | | | EXTREMELY IMPORTANT | | POOR / DISAGREE | ⟷ | | | / EXCELLENT |
| 1 | 2 | 3 | 4 | 5 | 1 Local PC and network passwords are updated frequently | 1 | 2 | 3 | 4 | 5 |
| 1 | 2 | 3 | 4 | 5 | 2 Network and local PC access are strictly controlled | 1 | 2 | 3 | 4 | 5 |
| 1 | 2 | 3 | 4 | 5 | 3 Access to update or amend marks on your student administration system, is controlled very strictly | 1 | 2 | 3 | 4 | 5 |
| 1 | 2 | 3 | 4 | 5 | 4 There is a clear and understandable policy for the capturing and amendment of marks | 1 | 2 | 3 | 4 | 5 |
| 1 | 2 | 3 | 4 | 5 | 5 Mark amendment audits are conducted frequently | 1 | 2 | 3 | 4 | 5 |
| 1 | 2 | 3 | 4 | 5 | 6 A very secure PC or server is needed to safeguard the exam papers on electronically before they are reproduced or written | 1 | 2 | 3 | 4 | 5 |
| 1 | 2 | 3 | 4 | 5 | 7 Your IT Department supports you in every aspect of information systems security regarding the administration of examinations | 1 | 2 | 3 | 4 | 5 |
| 1 | 2 | 3 | 4 | 5 | 8 Your IT Department warns and aids you in terms of technological vulnerabilities and security threats regarding the administration of examinations | 1 | 2 | 3 | 4 | 5 |
| 1 | 2 | 3 | 4 | 5 | 9 Your IT Department needs access to the PCs used to administer examinations on with the “Administrator password” | 1 | 2 | 3 | 4 | 5 |
| 1 | 2 | 3 | 4 | 5 | 10 Before examination papers are e-mailed between staff or departments they need to password protect the documents | 1 | 2 | 3 | 4 | 5 |

**SECTION C**

In the first three questions of this section you need to rate your Information technology or Information Systems department with regard to service levels. If you think they are EXCELLENT, circle the 5 or if you think they are VERY POOR circle 1 or any other number that represents your opinion between 1 and 5.

1 How would you rate your IT department in terms of support and reliability?

| Poor ← | | | | → Excellent |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

2 How would you rate your overall satisfaction with your IT Department?

| Poor ← | | | | → Excellent |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

3 How would you rate your IT department in the support and guidance they give you with the use of information technology for managing exam security at your institution?

| Poor ← | | | | → Excellent |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |



4 Are exam papers electronically distributed (e-mailed) between departments or staff?

| | |
|---|---|
| Yes | |
| No | |

5 **If yes** – What security is in place to support this practice?

| |
|---|
| |
| |
| |

6 Are exam papers stored electronically on a PC or server before being written?

| | |
|---|---|
| Yes | |
| No | |

7 **If yes** – What security is in place to support this practice?

| |
|---|
| |
| |
| |

8 **If no** – What form of storage is used e.g. Stiffy disks, removable storage devices (flash disks) or paper copies?

| |
|---|
| |
| |
| |

9 Is there additional network and / or PC security for the staff working with exams?

| | |
|---|---|
| Yes | |
| No | |

10 **If yes** – What security is in place to support this practice?

| |
|---|
| |
| |
| |

11 **If no** – Why not?

| |
|---|
| |
| |
| |

12 List the risk factors surrounding the use / abuse or absence of information systems to manage the administration of examinations at your institution. e.g. question papers are being e-mailed between departments without password protecting the documents.

| |
|---|
| |
| |
| |
| |
| |
| |
| |



13 How would you improve the examination processes using information systems as support mechanism e.g. submitting the examination questions on a web page?

| |
|---|
| |
| |
| |
| |
| |
| |
| |

14 Had there ever been a breach of security where exam papers leaked out or any other sort of exposed vulnerability that you know of? Please elaborate

| |
|---|
| |
| |
| |
| |