Title of Mini-Dissertation: Investigating the effectiveness of the access control system at Sol Plaatje University, in Kimberley, Northern Cape Province

Omogolo Paul Leepile Tlape

orcid.org: 0000-0003-4899-2996

Mini-dissertation submitted in fulfilment of the requirements for the degree *Master of Business Administration* at the North-West University

Supervisor: Prof. Jan Meyer

Examination: April 2019

Student number: 16864700

DECLARATION

I, **OMOGOLO PAUL LEEPILE TLAPE,** student number **16864700,** declare that this study titled, **"**Investigating the effectiveness of the access control system at Sol Plaatje University, in Kimberley, Northern Cape Province", is my own work and has never been submitted for any degree at any other university. All sources in this study have been indicated and acknowledged by means of direct and indirect references.

________________________ ________________________

Signed Date

DEDICATION

I dedicate this research paper with fondness to my wife, Catherine Tlape, my mother Mosadikago Tlape, my father Kebonethebe Tlape and siblings. They have always encouraged me to work hard at my studies and complete whatever I have started. I also dedicate this research paper to my late grandparents, Mr Okathusa and Mrs Kenyadiwe Monakwane and my daughters Maikano Tlape, Mosadikago Tlape and son Motlamedi Tlape.

AKNOWLEDGEMENTS

I wish to acknowledge with appreciation the following people:

- Professor Jan Meyer, my supervisor, for his strategic guidance and support during our interaction in crafting this research project; I appreciate the time given and efforts made on my behalf in this study;
- Dr Joseph Lekunze for all the assistance he gave me in acquiring some of the journal articles and his credible guidance in developing the questionnaire;
- My wife, Mrs Catherine Tlape, for her support and understanding;
- The language editor, Dr Jane Murray, for the support and input made in this study;
- Above all, I thank God Almighty for keeping me in good health and for sustaining me so I could complete this work.

INVESTIGATING THE EFFECTIVENESS OF THE ACCESS CONTROL SYSTEM AT SOL PLAATJE UNIVERSITY, KIMBERLEY, NORTHERN CAPE PROVINCE

ABSTRACT

The purpose of this study was to investigate the effectiveness of the access control system at Sol Plaatje University (SPU) in Kimberley, Northern Cape. Access control in various universities has been seen as a major concern by the management of these institutions and in other organisations. The key theory that underpinned this study was the system theory in access control management. The system theory is seen as an approach to access control in an organisation that guides many firms and institutions in access control management. The use of systems theory on access control management in this study could provide information to designers, developers, and access control professionals in an organisation on how access control can be managed in an organisation which operates as a system.

A mixed method research approach employing a sequential exploratory design was used. In this design, information obtained from the qualitative data was supplemented by the quantitative data. This allowed for triangulation and a comparison of respondents' and participants' responses in order to make sense of the study. For the qualitative part of the data, the researcher employed nine participants, which included two security managers and seven staff members at SPU. The quantitative part included 135 students in the five schools at SPU as respondents for the study. Data collection was done by means of semi-structured face-to-face interviews for the qualitative part and a self-administered hard-copy structured questionnaire for the quantitative part. The qualitative data was analyzed using content analysis while the quantitative data was analyzed using SPSS 24; a descriptive analysis was used to present the findings.

The main findings of this study revealed that SPU makes use of access control, such as cards and access management rules, to manage the access control system at the university. The study recommends that increased security and the use of a biometric system should be employed by universities and other organisations in order to enhance the effectiveness of access control management.

Key words: access; control; management; effectiveness; policy

Contents

ABBREVIATIONS

Abbreviation	Meaning
CUT	Central University of Technology
HEI	Higher Education Institution
ICT	information technology and communication
IT	information technology
NWU	North-West University
PIN	personal identification number
RFID	radio frequency Identification
RSA	Republic of South Africa
SABC	South African Broadcasting Corporation
SM	security manager
Sn	staff manager
SPU	Sol Plaatjie University
TUT	Tshwane University of Technology

CHAPTER ONE
OVERVIEW OF THE STUDY

1.1 INTRODUCTION

Organisations operate their businesses in an era where there is a high level of movement of individuals within the organisation. There are mechanisms that potentially could enhance the operation of an organisation depending on its alignment with the access of individuals in the organisation. One mechanism that should be considered in an organisation is its access control system. This study therefore focuses on investigating the access control system in universities and in particular, Sol Plaatje University (SPU).

SPU currently uses a proximity card system to manage the entrance and exit of people on campus. This access control system assists in monitoring the student and absenteeism of university employees as per the Basic Conditions of Employment Act, 1997 (Act No. 75 of 1997). The employee's proximity card is referred to as a staff card while for students it is known as a student card. The system is also intended to assist the security personnel in having exact data of the people on campus for reporting purposes. It is very important for an organisation, such as a higher education institution (HEI) to identify areas that need to be developed or improved in order to be competitive in the business arena (Sungau, 2013). Edmonds (2011) maintains that organisations should regularly review their goals and objectives, as well as their operating methods, in order to survive and remain relevant in the business arena. In summary, organisations need to be responsive to factors affecting their business.

Patrick (2013) affirms that securing a large college or university campus is a daunting task. Many campus police departments are stretched in dealing with crime, ranging from burglary to sexual assault, leaving them the resources to act only after a crime has been reported. Access control management solutions allow one to control, track and manage access to any facility for improved employee and visitor management. An access control system is effective in most universities but in others it is not effective. Hence, this study tends to investigate the effectiveness of access control management in SPU.

1.2 BACKGROUND

Under the new democratic dispensation three universities were established of which Sol Plaatje University (SPU) is one (Draft National Policy Framework for Public Participation, 2005). The other two universities are Sefako Makgatho Health Sciences University and University of Mpumalanga. In 2013 SPU was established by the South African democratic government (DoE, 2009). The formation of these new universities has the potential to enhance access to HEIs thereby contributing to one of the National Development Plan's goals, i.e. to increase Grade 12 education enrolment by 2030. This goal was also indicated on the Brand South Africa website when the former president, Jacob Zuma, stated that he foresaw an increase of enrolment in the country's HEIs from 17.9 per cent to 25 per cent in 2012 and 2030 respectively (SABC, 2017).

On 5 January 2017 the Brand SA website stated that in the year 2013 RSA had a total of 23 universities. They are disaggregated into 6 universities of technology, which focus on vocational-oriented education, six inclusive universities focusing on academic and vocational qualifications (diplomas and degrees), and 11 traditional universities focusing mainly on theoretical studies (https://www.brandsouthafrica.com/governance/education/south-africas-universities).

Previously there was no university in either the Northern Cape or Mpumalanga provinces. SPU started operating from existing building structures, formerly called the National Institute of Higher Education (NIHE) centre, that had been used as satellite campuses by North West University (NWU), Central University of Technology (CUT), and Free State University. Higher learning institutions instil knowledge and develop students to have the ability to participate in the economy of the country, and as such all these institutions need to have an effective access control policy that would secure both students and staff.

In addition, according to the SPU annual report, the university is at the consolidation stage of its development. It is the responsibility of the university's management and staff to ensure that there is minimal risk to the institution and to eradicate risks that could expose the institution to crime. Section 12 (b) of the Occupational Health and Safety Amendment Act, No. 181 of 1993 states that an employer must protect workers from hazards; where it is not possible to fully protect the employees from hazards the employer must minimise exposure to them.

It is important to continuously improve an institution’s administrative system, academic processes and access control management. The organisation should conduct business with unquestionable integrity, ethics and professional standards. SPU can achieve organisational efficiency and operational excellence and become a customer/student-driven organisation (Edmonds, 2011).

Patrick (2013) indicated that the login system of an institution needs to be programmed to disallow unregistered employees or students from entering the university. Managing access control effectively has the potential to reduce unplanned overtime, monitor absenteeism and reinforce the company’s human capital policies and relevant South African statutes. SPU is an academic institution and its access control system falls under information technology (IT) security.

1.3 RATIONALE OF THE STUDY

SPU has been selected for this stud because it is the only university in the Northern Cape situated in the capital city of the Northern Cape. During the 2015 academic year university students took to the street protesting against the increase of tuition fees at South African universities and demanding free education at universities under the theme “#fees must fall”. In the 2016 academic year, students continued their action after the Minister of Higher Education declared that an increase would be capped at 8% for the 2017 academic year.

Properties and assets valued at millions of rand were damaged due to the aftermath of the “#fees must fall” protests at South African universities. Many non-students gained access to various universities and damaged property. Security staff at these universities were surprised at the numbers of non-students who gained access to the university despite the high security provided.

Even though students at SPU protested in the “#fees must fall” campaign, no significant damage was experienced at the university. Non-students were seen around the buildings but could not gain access to it. This study intends to investigate the access control strategy used at SPU in order to ensure that university property is secured.

The outcome of this study will

- Measure the level of effectiveness of the access control system of SPU;
- Inspect the relevance of the access control strategy of SPU;
- Study the link between the strategy, reporting and accountability of the access control system; and
- Assist to monitor the implementation and effectiveness of the access control system.

1.4 PROBLEM STATEMENT AND CORE RESEARCH QUESTION

Access control management is one of the measures that play a significant role in the daily operation of a business. There are many types of access control systems that can be used in the market and organisations can select the most appropriate system depending on their size in terms of human capital, budget allocated for development and maintenance and management of the access control system. Lastly, the system must achieve the desired needs. Some of the challenges faced by organisations are absenteeism and forging daily duty reports in the register. Companies that lack an access control system face the challenge of prohibited people entering the companies' premises, which compromises security.

Muhammad et al. (2014) indicated that web-based scientific applications that are used in an organisation provide a way of sharing scientific data beyond the local computing environment. The organisation and sharing of large and heterogeneous data pose challenges due to their sensitive nature. There is a need for a robust authorisation mechanism to prevent unauthorized access to an organisation.

Edmonds (2011) also indicated that universities can be exposed to problems relating to attack from an insider. An insider attack is someone using access to an organization to violate protocol or cause harm intentionally or unintentionally. Many institutions fell prey to this situation during the fees must fall context. Access authentication, such as the use of a student or staff card, is required in most scenarios, because only authenticated and authorized student are able to access a network. This system has not been closely monitored or been seen as effective because universities still face challenges on the exchange of cards from one student another in order to gain access. Hence there is a problem on managing security when thousands of visitors enter and leave the university premises each day and the premises have to be protected against intrusion, theft and vandalism on distributed properties covering acres of land (SOLUS, 2016).

Although there have been studies conducted in relation to internet access control in general, at this juncture there is no study that was performed to gauge the effectiveness of the access control system at SPU. The effectiveness of the system is characterised by the proper usage of the access control system in place and the strategies deployed to ensure compliance and level of effectiveness. The problem faced in the access control system of the organisation is the poor management of its performance. This factor can be identified as a lack of accurate reporting of errors that occur and data administration. These are matters of concern for the designated official/s and management who are required to take responsibility for the improvement of outcomes of access control. Hence, this study investigates the effectiveness of access control management at SPU.

Research questions:

The following research questions will be asked in this study:

- What is the access control policy management used in SPU?
- What are the challenges faced by SPU in access control management?
- What are the perceptions of students and management on the access control management used at SPU?
- How effective is the access control policy management at SPU?
- In what way(s) can access control management be improved at universities?

1.5 RESEARCH OBJECTIVES

The research objectives of this study are to:

- Investigate the access control policy management used at SPU;
- Examine the challenges faced by SPU in access control management;
- Examine the perceptions of students and management on the access control management used at SPU;

- Investigate the effectiveness of the access control policy management used at SPU;
- Investigate way(s) the access control management could be improved at SPU.

1.6 IMPORTANCE AND BENEFITS OF THE PROPOSED STUDY

The proposed study has the potential to assist decision makers when they review their access control systems. It is important for companies to review their plans and implementation processes in order to improve their services and to be competitive in the market. This study will show how information, technology and communication (ICT) contributes, in particular IT security, and how it can affect the operation of a business. SPU is an academic institution and with regards to their access control system the institution uses the access card. This study will look at the advantages of the access card, level of effectiveness of the access control system of other access control systems in the market and how to enhance the access control system of the university.

The access card control system has the potential to minimise, if not to eliminate, unauthorised entry to the premises of the university. The other issue with the system is that it makes the reporting process simpler; management can detect the number of employees and students on campus. The access control system needs to be monitored and evaluated on a regular basis in order to enhance its ability to produce the desired outcome.

1.7 DELIMITATIONS

The study of investigating the effectiveness of the access control system will be conducted only at SPU, Kimberley in the Northern Cape Province. The access card system that is implemented at SPU is the access card control system. Participants who are going to complete the questionnaire are employees and students from SPU.

1.8 SUMMARY

This chapter presented the purpose of the research and the background dealing with changes envisaged in higher education in terms of universities in the Republic of

South Africa and the importance of the access control system. The problem statement states that institutions that lack an access control system face the challenge of prohibited people entering the companies' premises and that compromises security of information, assets and legitimate people who are permitted on the premises. Additionally, the primary and secondary research objectives are to evaluate the use and management of the access control system and to evaluate the effectiveness of access control in the implementation of the access card system respectively. The proposed study has the potential to assist decision makers when they review their access control system.

1.9 RESEARCH LAYOUT

The dissertation is presented in five chapters.

Chapter one of this research outlines an overview and orientation of the study.

Chapter two will examine the theoretical foundations of related research. It provides an overview of access control management, its challenges and effectiveness in an organization.

Chapter three will explore the qualitative and quantitative elements of the research methodology. The methodologies and techniques that will be used in the collection and analyses of data will also be discussed in this chapter.

Chapter four will present the results and findings of the research. The research questions are discussed in detail, and the reliability and validity of the research will also be explored.

Chapter five will combine all the previous work into a conclusion of the results with recommendations for future research. This dissertation aims to identify the effectiveness of access control management in SPU.

CHAPTER TWO
LITERATURE REVIEW

2.1 INTRODUCTION

In the previous chapter, an overview of the study was made. The background of the study, research problem and research questions and objectives were outlined. In this chapter a review of relevant literatures in relation to the study will be made. The purpose of reviewing the relevant literature is to enable the researcher to view what other researchers have found in relation to the study and also to identify the gap from other studies that needs to be filled.

2.2 ACCESS CONTROL THEORY

Theoretical framework not only described the structure that can hold or support the theory of a research study, but also introduces and describes the theory that explains why the research problems under study exist. Therefore, for the readers as well as the researcher, to obtain in-depth understanding of the topic, the researcher will use the “system theory on access control”.

According to Conklin and Dietrich (2008), systems theory has been applied to many areas of study and systems-engineering approaches have guided many firms in their access control management. Systems theory in the management of access control can be seen as the process followed by an organisation in order to ensure that the access control or security management are well managed as a system within the organisation. Cavusoglu et al. (2012) argued that the importance of security and access control is echoed by reports from organisation and industry groups, but as the importance is placed at the entire system or enterprise level, the solutions that are employed are at a single specific system level. Abadi et al. (2014) also argued that technologies have been developed to combat specific levels of access control threats that occur in a system. These threats can be divided into a range of different categories, such as network attacks, operating system attacks, social (people) attacks, and application level attacks. The use of systems theory on access control management in this way will provide information to designers, developers, and access control professionals in an organisation on how the management of access control can be done in an organisation which operates as a system.

2.3 OVERVIEW ON ACCESS CONTROL SYSTEM IN SPU

The Higher Education Act of 1997 (No.101 of 1997) guided the process to establish public universities. In the aim of establishing public universities, SPU which had provisionally been referred to as the University of the Northern Cape was declared by the Minister of Higher Education (HE) in the government notice 630 dated 22 August 2013 as a public university. After the official launch of the university in 2013 as a public institution, it opened its doors in 2014 by registering 135 students. According to SPU's website, the university currently (2016) offers 8 qualifications from 4 faculties. These qualifications are as follows: 5 bachelor degrees, 2 diplomas and 1 certificate.

In terms of the access control system, SPU uses an access card for the purpose of entering and exiting the premises by staff, students and visitors. Further investigation should be done to measure the effectiveness of the access control system at SPU. In this paper the focus is on investigating the effectiveness of the access control system at SPU.

The next section will give an overview on the access control system in an organisation. This would enable the researcher to have a clearer view on how organisations operate.

2.4 OVERVIEW OF ACCESS CONTROL IN ORGANISATIONS

Organisations operate in a very competitive and challenging business environment; one of the challenges is to manage access of workers and other stakeholders into and out of the organisation's premises or systems. In this day and age access control is implemented in almost all aspects that are involved in the business environment, e.g. the company's premises, financial systems, human resource systems, and storage facilities. Khan (2012) argued that access control systems are becoming more sophisticated because of new innovative developments in the field of access control, mostly among companies. There is therefore a need for sufficient safety of information, assets and people and is an essential task for management in organisations (Hu et al., 2006).

In addition, access control is a technique of regulating and reporting on individuals who enter and exit the organisation's premises with the knowledge of the purpose of their entry (Hu et al., 2006). Kuhn et al. (2010) agree with Hu et al. (2006) by indicating that access control can also be defined as a mechanism that permits or prohibits a person the right of entry to a specific location. This means that one of the functions of access control is to trace or record the number of people going in and out and to know their motive and their whereabouts within the jurisdiction of the organisation. Those records can be used as data trails when performing audits or monitoring compliance.

Furthermore, access can imply to consume, utilize or to go into (Hu et al., 2006). The access control system must determine who can enter, when and where. The system is utilized in order to improve safety and allow people with rights to gain access to do so. It is important for an access control system to record the name of the individual, contact details, time of entry and exit of the premises. This information helps management to make informed decisions.

There are different types of access control systems that can be deployed in order to manage access of individuals. Those access controls are either manual access control or electronic. Manual access control systems are in the form of a physical key and logbook register while the electronic access control systems are keypad, smartcard and biometric access control system (Teh et al., 2013). To a certain degree the manual access control system has limited capability to obtain the entire purpose. On the other hand, the electronic access control system is being advanced through continuous research. Currently, information technology is advancing the way organisations operate their businesses.

According to Teh *et al.* (2013) the electronic access control systems utilise an access control reader that match the correct electronic key (pin, card or body part) with the data that is stored in the database. The access control reader is linked with the database and the specific door or gate. The access reader allows the gate or door to open when the electronic key links with the data from the database. Fencing complements access control system because it restricts individuals from entering the location without permission; it rather leads people to look for an entry point and in most cases gates have access control systems. The access control reader needs to be monitored to ensure that no unofficial person fiddles with the device and compromises its credibility.

A proper access control system in organisations is indispensable and meant to make users accountable for their acts since they can be monitored. It also does not allow an individual to abuse the system. The purpose of access control is to determine the allowed entry or activity for a genuine user. To a certain degree, the safety of all stakeholders (employees and other stakeholders), assets and information in the company depend on the system. Access control has a broad range of characteristics; its administrative ability and functioning of the system are the most important aspects (Hu et al., 2006). The functioning part of the system has many inputs; the access-controlled door is one of them (Khan, 2012).

Hu et al. (2006) highlighted three aspects to look into when developing and implementing an access control system, i.e. access control policy, model and mechanism. Access control policy serves the purpose of providing guidelines as to which access control system to adopt, who must be granted access, where, when, how, and also provide guidance as to how to manage the access control system. Thereafter, access control is put into effect using a mechanism that communicates the validity of the entry request by the user.

Access control plays a role of linking the gap between policy and mechanism. Hu et al. (2006) further explained that one of the policies related to an access control system policy is the security policy, which must be enforced through a system and determine limitations. Maximum freedom to access every entry of the organisation could result in unauthorised entrance (Hu et al., 2006).

Access control policies differ from one company to the other depending on their objectives. Businesses operate in a very competitive environment; therefore, access control policies should be reviewed regularly to complement the organisation’s objectives at that time. There are two access control policies; the first is discretionary policy, which is in relation with uniqueness-based access control; and the second is a non-discretionary policy which is concerned with how to regulate access control

(Hu et al., 2006). Patil el al. (2012) indicated that the discretionary policy regulates the users' access information whereby access can be given to users based on their identification. The discretionary policy states individuals who can gain access to the organisation and who should access information of the access control system in the database (Patil el al., 2012).

Private and public entities depend on data processing systems because those systems have to achieve the operational and financial obligations of the organisation, together with their reports that should be performed with ease (Ferraiolo et al., 1992). Therefore, the reliability, accessibility and privacy of the data in the database should not be compromised. If access control is not managed optimally, fraud can be easily committed, and theft of the organisation's possessions (i.e. furniture, machinery and other assets) could interfere with the functioning of the entity. As a result, the organisation would experience a lack of resources and be faced with financial crises; lastly, the safety of workers and other stakeholders would be compromised. It can be deduced that organisations are implementing access control in their organisations. As such, there is need to review the importance of these access control mechanisms in an organisation. The next section will review the importance of access control in an organisation.

2.5 RELEVANCE OF ACCESS CONTROL STRATEGY

Hu et al.(2006) mentioned the following aspects of access control. The safety of an organisation's belongings can be guaranteed if the access control system is reinforced in such a manner that no unauthorised individual will be allowed access. Suppose the unauthorised individual gains access, misuses the company's belongings and manages to exit without being identified as an intruder, no one would be accountable for the damage. The access control system will not be serving its purpose to its optimum level. From a business point of view, access control is one way of regulating the issue of using and sharing resources and information.

A properly regulated access control system can classify sharing of information according to the rank of the user but when that mechanism does not exist sharing of information can be unmanageable. For example, a worker who is responsible to administer the server room facilities must be granted the privilege to access the server room in order to perform his or her enforced duties within that area. This person should have limited access only; not access to other areas in the company, e.g. the financial archive area. The access control system helps organisations to make every individual involved in a specific operation of the business accountable.

The access control system advocates the segregation of duties because if it is regulated appropriately, the limitation of access will make it possible for all individuals to focus on the activity that they must perform. One example could be the finance unit where one person has access to collect revenue from clients, another person is allowed to bank the money, while the third will have authority for the reconciliation of financial records. A well-managed access control system has the ability to reduce irregular and wasteful activities that cost the organisation a great deal of money. The organisation needs to craft a hierarchy that determines the authorisation of individuals' access to the entry points of the organisation.

Kuhn et al. (2010) argued that appropriate functioning of the access control system requires that the responsibilities of individuals are within one unit. According to Sandhu et al. (1996), segregation of duties can be imposed in two different ways, i.e. statistically or dynamically. Statistically is by determining conflicting roles like responsibilities that cannot be performed by one worker, while dynamically is by enforcing the regulation at access time.

In multiple activities there should be an accepted hierarchy of responsibility, based on principles of speciality (Sandhu et al*.,* 1996). This means that an employee (scientist) who is given responsibility to work in a particular laboratory will be given the privileges to access that laboratory in order to perform the duties assigned to that worker; whereas the supervisor of laboratories will be granted access to all the laboratories. On the other hand, the accounting officer of the institution will inherit the right to access almost every section within the organisation. Hierarchical responsibilities make authorisation administration simple (Sandhu et al., 1996).

Work responsibilities determine the degree of privileges the employee should inherit when it comes to accessing the organisation's sections. Supervisors and management officials are allowed more privileges to access points in the

organisation compared to their subordinates and they should implement them only when there is a need (Sandhu et al., 1996). For example, supervisors should visit all sub-units under their supervision to monitor progress while management officials visit all units for official rounds. The limitations of access privileges reduce the threat of misusing access and decreasing unintentional mistakes or an intruder pretending to be a genuine user (Sandhu et al., 1996). Hence, there are policies and related statutes that shed greater light on the use of access control in an organisation.
The next section will review these policies in relation to the study under review.

2.6 ACCESS CONTROL POLICY AND RELATED STATUTES

Access control mechanisms respond and mitigate the challenge of trespassing. The South African Trespass Act of 1959 (Act No. 6 of 1959) serves the purpose of preventing individuals without any authorisation under certain conditions to enter land and buildings. The South African Trespass Act of 1959 (Act No. 6 of 1959) states that an individual who is permitted to enter land in accordance with the Extension of Security of Tenure Act 1997 (Act No 62 of 1997) will be believed to have a legitimate motive to gain access and be within that land. Therefore it is important for every individual who seeks to gain access to someone's or the organisation's land and building to request permission and the access control system plays a pivotal role in ensuring that access is permitted and that the individual's request was authorised.

Institutions with an access control system or intending to put access control in place need to consider developing an access control policy (Hu et al., 2006). The access control policy provides firm access control guiding principles that need to be adhered to during implementation. To have a successful access control system, access control policy is required since it highlights the purpose of the system and specifies the objective with reference to the needs of the organisation. The access control policy will also state how to regulate access, who can gain access, and under what conditions access can be granted. An unmanaged access control system could make the possibility of unauthorised entry simple, and that would attract those with criminal intentions and legitimate users to abuse the privileges.

The next section will highlight various access control management systems used in organisations as well as the advantages and disadvantages of these systems.

2.7 ACCESS CONTROL MANAGEMENT USED IN ORGANISATIONS

In this day and age, everywhere one goes there is access control; at border gates of countries, gates and doors of organisations, and so on (Hu et al., 2006). Most of the time organisations employ security guards to monitor the entry and exit of individuals. When the access control system is manual the security guard will be on hand on to verify the identity of the individual; registering all the necessary information needed like the name of the visitor, time of entry, purpose of the visit after which access is granted. When the access control system is electronic the security guard will be on duty to ensure no one abuses the privilege of gaining access to the institution; and to report on time when the access control device gives problems (Tong et al., 2011).

Hu et al. (2006) identified three access management methods. The discretionary access control method allows the administrator of the access control system to grant access privileges to the organisation or buildings within it, based on his or her discretion. The second method is the mandatory access control method; with this method the access control operation system is programmed to make a decision whether to grant access or not based on the information that is saved for verification. As a result, the owner or administrator has a smaller workload since the system does most of the work. The mandatory system, on the other hand, classifies individuals. The rules that determine who should gain access are documented in the access control policy and the security policy. Both policies are developed by management and must be aligned with the objective of the institution (Hu et al., 2006).

Sandhu et al. (1996) indicated that the access control policy and the security policy are put into effect by the access control system that is made possible by the IT security. The mandatory access control method is authoritarian compared to discretionary access control. The third access management method is role-based access control; with this model the individuals are given access to the organisation's premises based on the responsibilities they have been given in the organisation. Role-based access control is a non-discretionary access control because individuals

gain access privileges based on their responsibilities. Companies need to choose their method based on what they want to achieve and their type of business.
The role-based access control method is most favoured when a company has few users and a limited worker turnover (Sandhu et al., 1996). The issue of attaching access rights to work responsibilities eases the work of the access control administrator when it comes to managing access points. Role-based access control makes the utilisation of limited access privileges standard and helps the company to comply with tight regulatory principles (Sandhu et al., 1996). If the correct measures of role-based access control are not properly implemented the entire rationale behind the method serves no purpose (Sandhu et al., 1996).

In addition to the access control methods identified by Sandhu et al. (1996), the following was also identified in literature as part of access control management that could be used by an organisation.

2.7.1 Smart card access control system

According to Nixon et al. (2015), a smart card is mostly used in the banking industry, by universities and when buying with credit. At the bank, account holders use smart card to access their monies from the automated teller machine (ATM). At universities both students and workers utilise cards to enter campus and building, while at retail stores individuals with an account at a particular store can use their credit card to buy the desired items and pay later. Figure 2.1 shows the management of the smart card system.

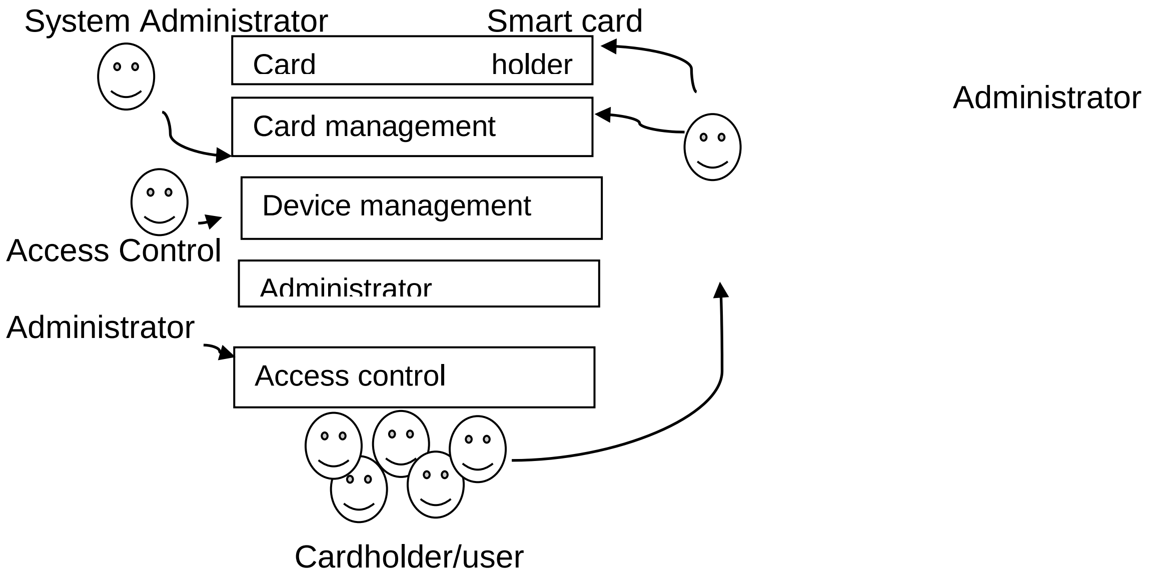


Figure 2.1: Management of smart card system

Source: (Tong et al., 2011 in Nixon et al., 2015)

Figure 2.1 illustrates that data from administrator management and access control are saved in both the database and the smart card. The cardholder brings the smart card to the smart card administrator when there is a problem with the card or when there are any changes to it. The system administrator is responsible for monitoring the smart card device. If there is fault with the device it is the responsibility of the system administrator to resolve the problem or report the matter to the relevant official. This system is used by many organisations that are sceptical of managing an effective access control system.

2.7.2 Biometric access control system

The word biometric comes from the Greek words “bio” and “metrics” meaning “life” and to “measure” respectively, that is according to biometric update website. Biometrics is an essential element of identity science and commonly used in the IT security field for the purpose of recognizing people (Nigam et al., 2015). The first biometric used was called soft biometrics established by Bertillon in the nineteenth century (Nixon et al., 2015). Later in the early twentieth century a biometric system using fingerprints was established; from there more studies revolving around biometrics were conducted (Lumini et al., 2016). Innovation has played a critical role in advancing the field of biometric access control; more than one feature of a human body can be used to validate access (Nixon et al., 2015).

Teh et al. (2013) highlighted that the biometric access control system includes network access control, which enables someone to gain entrance to a building, identity management control, web management control or remote access control. According to Monwar et al. (2009), the biometric system has the latest technological features to authenticate a person's identity. Biometric access control has the ability to protect the integrity of personal information, verify an individual's details and the potential to eliminate or prevent theft and fraud (Monwar et al., 2009). This is made possible by the growing ICT environment because every day there are innovative initiatives on how to enhance IT solutions that improve the lives of people and entities using technology. Technology in the working environment assists in enhancing the performance of an organisation in order to achieve its desired outcomes (Monwar et al., 2009). The improvement that comes with technology makes operations, systems and machinery effective, efficient and user-friendly. The biometric access control system has a safety feature that detects and manages the genuineness of an individual's fingerprint, in and out of the premises (Tuyls et al., 2006).

Teh et al. (2013) argue that the biometric access control system not only manages the access of individuals in and out of the particular premises, but also has the potential to reduce, if not eliminate, a break in by unauthorised intruders since the biometric system is an advanced access control technique. The electronic access control system offers a safer option in safekeeping the jurisdiction of an organisation. Access control is one method developed and implemented to manage channels of entrance and exit in particular premises (Teh et al., 2013).

Biometrics is a developing arena within the information communication and technology (ICT) industry dedicated to identifying an individual through scanning biological characters like fingerprints, iris or face (Riera et al., 2008). Wayman (2001) further stated that there are no boundaries in biometrics when identifying and authenticating characters of a human being; the following can be used: hand, face, foot, finger or thumb, ear, eye and voice.

Gafurov et al. (2006) stated that a biometric system functions through obtaining biometric information from a person who is seeking access and links that information with one that was previously captured and saved for verification in the database. The information that is scanned when seeking access is the verification sample; if it matches the information in the database the individual will be allowed access and when the information does not match the individual will be denied access. Therefore, when an individual submits information requesting access it can be identified as genuine or fake data (Gafurov et al., 2006). Therefore, it can be deduced from the above literature that the biometric access control system provides a trustworthy resolution and is reliable and effective when it comes to authenticating identity.

In addition, Bharadwaj et al. (2015) defined the biometric system as a mechanism that has the ability to identify the validity of a person using body features, e.g. the iris, face or fingerprint. Other scholars, e.g. Lumini et al. (2016) defined the biometric system as a technology implemented to identify and verify an individual's unique physical features or interactive characteristics which provide an essential substitute to the manual access register book, smart card or password. The biometric system stores information in the database and nowadays organisations depend on that system to enhance security at entry points of institutions.

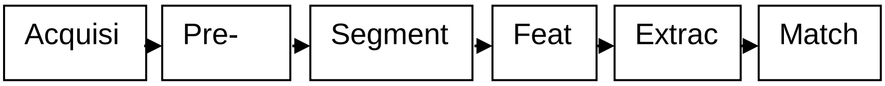
Bednarek et al. (2013) also stated the purpose of the biometric access control system; it strive to guarantee an optimum level of security and deliver a system that is convenient to be implemented by the user. For the biometric system to be a conventional method of managing access, its developers will have to show and prove that those systems are tough and have minimum error occurrence (Anil et al., 2008). A biometric access control system implements security settings and regulates access rights to manage access points at a particular time (Bednarek et al., 2013). According to Li et al. (2010), biometric characters cannot be misplaced or forgotten because they are part of the user; it is difficult for the user to share his or her unique characters with another person; it is difficult to forge biometric characters; one cannot disseminate the biometric key of an individual for use by multiple users. As such, management in an organisation needs a mechanism that can assist them to make appropriate decisions.

The biometric access control system has the potential to provide accurate information when it comes to matters relating to absenteeism, late coming, and overtime work of employees (Javier et al., 2014). Authentic information can assist decision-makers to improve productivity in the company (Javier et al., 2014). That can only happen when a suitable access control system is implemented, regularly monitored and evaluated. Workers need to understand the importance of the fingerprint access control system and adhere to the information that is provided by the system administrator in order for it to produce positive results. Those positive outcomes can result in a decrease of unauthorised absenteeism and an increase in productivity.

In previous years many industries experienced positive results from the biometric system and the system is still providing one of the best security features for access control (Meraomia et al., 2011). The biometric system is implemented to manage immigration and crime (Venkatraman et al., 2008). In South Africa (SA) the Department of Home Affairs uses fingerprints to authenticate citizenship and identify illegal immigrants and the South African Police Service (SAPS) uses fingerprints to link the perpetrator with the committed crime. The biometric system also decreases the theft of identification (Bhargav-Spantzel et al., 2006). Security in the workplace needs to be intensified hence it is important to protect an individual's identification (Verkatranman et al., 2008).

Studying the effectiveness of the access control system in the case of this study is pivotal because the outcome of the study will determine whether the system is achieving the objective that was set. For example, is the system sufficiently reliable to achieve the set desired outcomes? The effectiveness of the electronic access control system relies on the quality of the system and the implemented authentication technique (Gafurov et al., 2006). On the other hand, Wayman (2001) determines the effectiveness of the access control system by inspecting the identification, authentication and authorisation techniques.

The system must be able to do the following: (i) determine the identity of a person in the database; (ii) verify the data submitted to the database; (iii) authenticate the right individual. After identifying and authenticating the individual, the system must register and save all the required information and allow that individual access. That exercise is performed with minimum security. Figure 2.1 shows the systematic flow of data in the biometric device.



Source: Nigam et al. (2015)

Figure 2.2: Systematic flow of data in the biometric device

Scholars have investigated many types of acquisition techniques using human characteristics (Nigam et al., 2015). There are different methods, tools and also required space at which the specified human characteristics have to be placed on the device for capturing. When the required body part is placed on the biometric device the features of that body part are captured by the device. For example, if it is the palm of the hand that is required, the device takes particular features of that palm and matches them with those in the database. Only when there is a match will access be granted but when the presented features do not link with those in the database, access will be denied.

Lumini et al. (2016) highlighted that there are various environmental issues that could tamper with the flow operation of the biometric system, e.g. moisture, weather conditions, etc. The performance of the biometric system can be affected by the quality of inputs used, e.g. the sensor, durability of the system and loading data beyond the predetermined quantity. The use of a biometric system demands sensitive care and is the latest trusted method of managing access at entry points.
Lumni et al. (2016) also stated ways to measure the performance and the accuracy of the biometric system, i.e. capturing sample error of the system and the rate at which the system fails to recognize the user. Sample error is the rate at which the system initially failed to capture the user sample correctly in the database. It can be caused by the poor or incorrect inputs used in the system. Failure of recognition is caused by the quality of the individual’s key characteristics as presented and that could be due to exposure to environmental issues or the device’s exposure to dirt. As a result, correct measures must be taken when capturing the credentials of an individual.

It is therefore important to determine and gauge the accuracy of the system when matching the biometric data of the user with that in the database. This would ensure that the right users are currently using the database system. Lumni et al. (2016) and Hu et al. (2006) identified the components of four groups that can be quantified. The first group consists of a correct acceptance rate, correct match rate and accurate positive acceptance. These measures are the proportion of the valid matches which the biometric system managed to correctly link from the data from the database to that of the user. The rate of those components must be maximized all the times.

The second group of components is an incorrect acceptance rate, incorrect match rate and incorrect positive. These components are measures when the system validates an incorrect identity and that should be minimized. The third group of components comprises a correct rejection rate, correct non-match rate and correct negative. These measures occur when the biometric data from the database is not linked correctly with the individual's feature/s; in brief, the user's information is not stored in the database and the measures of those components must be increased. The fourth group components include an untrue rejection rate, untrue non-match rate and untrue negative. These measures occur when the biometric system does not recognize the details of the user whose details are stored in the database. Those measures must be minimized. The database is the critical element of data administration of the daily functioning of the access control system with which decision-making has tremendously improved together with the safety of the data administered (Patil el al., 2012).

Therefore, knowing the accuracy status of the system will assist the decision-makers to identify areas to be improved from the very same system in order to enhance the credibility of the biometric system. Improvement in the biometrics arena is driven by innovative individuals with the technical knowhow revolving around IT security. According to Hu et al. (2006), it is simpler and possible to make information obtainable through the use of information technology. This is made possible by the record stored in the database and it can be saved in a systematic manner. The system must be able to identify the number of people who gained access, categorize the nature of their access (workers, students, visitors 'official or non-official', suppliers, etc.) and the exact time of entry and exit. Suppose a catastrophic event occurs, e.g. the building catching on fire or building structure collapsing, information can be retrieved from the system to identify who was in the building during that act. This study is therefore aimed at investigating the effectiveness of the various biometric access control management systems used in universities.

2.7.2.1 Advantage of using the biometric access control system

According to Riera et al. (2008), biometrics has become an area that is mostly researched in IT security since the biometric access control system is considered reliable and requires less physical security. The biometric access control system has a low occurrence of errors when compared with other options. The system is user-friendly, no external object/s is required to gain access, and it can be developed to require a fingerprint, palm of a hand or iris of an eye, depending on the specifications of the organisation (Teh et al., 2013). The system is environmentally friendly since it is digital and eliminates paperwork as workers do not use a register or timesheet to enter their details in order to gain access (Bednarek et al., 2013).

The system eliminates the issue of forgetting, forging, misplacing the physical key, card or password. In other words, the identified data of an individual's characteristics (e.g. fingerprint) is obtained and saved in the database. When that person requires access the only thing that is needed is to present the saved features to the device that manage access (Teh et al., 2013). The biometric system is one step ahead when it comes to reducing if not eradicating cases of criminals or intruders who steal keys, cards and forge passwords in order to gain access. According to Khan et al. (2007), the biometric system remains the preferred mechanism to reinforce security at access points.

In addition, the biometric access control system has the ability to reinforce access security to the jurisdiction of an organisation (Bednarek et al., 2013). Every individual has the responsibility to take care of the resources to which he or she has access. The biometric system can determine and provide a report as to when and where those particular individuals gained access. Therefore the system enhances the issue of accountability. The biometric system has the potential to eliminate human error in a working environment when it comes to registering access of employees into and out of the organisation’s jurisdiction (Bharadwaj et al., 2015).

2.7.2.2 Disadvantage of using biometric access control system

Even though the biometric access control system has minimum error occurrence, there is also a slight chance of error (Anil et al., 2008). The error occurrence can be due to saving the incorrect identity of an individual; as a result it might allow access to the wrong user. The other error occurrence can be when the legitimate users are denied access by not validating their identity. These error occurrences are mainly caused by the system itself or by the administrator. All the biometric access systems available in an organisation have their unique merits and demerits (Chung, 2001). An example can be made using a fingerprint device. With reference to the construction site or factory where the fingers are exposed to moisture, oil, mud or dirt, in general the fingerprint device can find it difficult to verify the data of individuals who seek access.

2.7.2.3 Solutions driven by the biometric access control system

An organisation that deploys an unreliable access control system or does not manage the access of employees in the working environment has the strong possibility of facing the following challenges:

- Paying employees who do not come to work;
- Decreased productivity because of employee absenteeism:
- Late arrival of employees;
- Employees taking long lunch breaks;
- Workers register absent colleagues;
- Supervisors’ failure to report unauthorised absenteeism;
- Inconsistent or unreliable clock-in register.

In this regard, decision-makers could be misled by that information. All these challenges could cost the organisation loss of funds and other resources and harm the integrity and credibility of the company (Teh et al., 2013).

The solution to these challenges would be to develop a policy that complements the use of a biometric access control system. That system has the potential to eradicate or minimise the challenges faced by the organisation due to poor management of the employees’ clock-in register. By contrast, a biometric access control system has the potential to capture the time and the user’s details accurately and then generate a reliable and credible report for decision-makers (Bednarek et al., 2013). The system can generate the report instantly (Teh et al., 2013). The biometric system does a tremendous job because supervisors spend less energy and time in processing the access register of employees for decision-making (Bharadwaj et al., 2015).

Because an individual has unique characteristics on the fingerprint, iris or palm of a hand, the biometric system has the potential to eliminate the use of a single identity by more than one user (Wayman, 2001). Through continuous research in the field of biometrics in IT security, the misapplication of access control will be a thing of the past as the access control is advanced in its use of technology. Biometrics has advanced the field of IT security in the working environment.

2.7.3 Human security method

In addition to the smart card access control and biometric access control, schools and HEIs employ other forms of access control management, such as human security access control. This type of access control management involves the use of guards, community and/or parental participation, school personnel, security officers, private security company personnel on contract who might also offer a rapid armed response service, or police officers. According to Bitzer and Hoffman (2007), the human element in security systems is often overlooked or neglected completely in literature on the subject. However, it plays a vital role in security. It is usually humans that make the decision to take action and decide on what action to take during a crisis or emergency (Bitzer & Hoffman, 2007). Most technological measures will not be able to function successfully without a human component. For example, if a biometric access control system or smart card is triggered at an organisation, a policeman or security guard will have to respond in order for the technological aid to work effectively and to apprehend any intruder.

Human security measures expect guards and security officers to patrol the premises, inspecting and observing the activities taking place and the locations where incidents occur in order to identify any risks. Part of patrolling duties also include identifying shortcomings or damage to a security measure (e.g. hole in a fence) or whether a system is operational (working properly). Having these human security measures on the premises might decrease the fear of crime on the part of students, staffs and parents, as well as assist with the prevention of crime (Lombaard & Kole, 2008). It is therefore vital that the human aspect of security is not overlooked or neglected, but that it is fully utilised and integrated with the technology and security equipment available.

2.7.4 Policies and procedures

Along with other methods used to manage the security of an organisation, policies and procedures need to be in place. Policies are the goals and objectives that the organisation wants to achieve and therefore assist with decision-making (Rogers & Schoeman, 2010). Procedures are the 'guidelines' that inform everybody how the objectives in the policy should be carried out and provide instructions on how security activities should be conducted. Policies and procedures are a vital part of the security system at any institution. They set guidelines and provide direction as to how situations should be effectively managed and handled (Rogers & Schoeman, 2010). The policy clearly states what the authority of the various people is and what the limitations or restrictions of those individuals are in the institution. The policy of an institution should also reflect its access control management. This is because both security policies and procedures are relatively inexpensive measures that can be used to assist with the solution and reduction of crime and violence on the premises.

In drafting this policy, it is important to consider the aspect of zero-tolerance. Zero-tolerance policies were put into place in the mid-1990s after great increases in school and university violence (McAndrews, 2001). These policies deal with problems relating to school safety and discipline and state that no violence, crime or any other unauthorised activities will be tolerated. Those who violate the policies will be punished. The importance of having zero-tolerance policies in place and for them to be effective is that they should be taken seriously by students and staff members and the consequences must be consistently enforced (Lawrence, 2007). Even though there has been much debate and arguments on zero-tolerance policies, some researchers and institutions have found them effective while others state that zero tolerance has not shown an improvement in the safety of an institution and that it has largely been ineffective in institutions (Graves & Mirsky, 2007). McAndrews (2001) argued that some institutions and high schools in Washington DC and New Jersey in USA, implemented zero-tolerance policies against fighting (on school premises) in 1991 and within a year there was a 95% drop in violent behaviour, such as damage to school properties and the access of non-students into the institutions. Critics feel that there have not been sufficient studies done to test the effectiveness and impact of implemented zero-tolerance policies in schools but institutions and various organisations should continue to implement the policies on zero-tolerance in order to achieve effective access control in an institution.

Management in an organisation needs to ensure that the access control measures identified above are effectively used in an organisation. Hence the next section will help to shed more light on the effectiveness of the access control management used in an organisation.

2.8 EFFECTIVENESS OF ACCESS CONTROL USED BY MANAGEMENT

Sandhu et al. (1996:20) stated the following: “In order for the access control system to be effective, it must provide an appropriate user identity and on the accuracy of the authorisations it needs to regulate access of individuals”. It is indispensable to realise that access control is not an absolute solution when it comes to protecting the assets, information or workers in the jurisdiction of the organisation although to a certain degree it plays a role of safety. The effectiveness of access control is based on the processes used in an organisation. They include authentication, authorization and audit. With regard to authentication, every business implements authentication to one extent or another. Credentials may include a simple user name and password, or more sophisticated authentication like a smart card and PIN. Authorization, on the other hand, allows users access to the appropriate applications, servers, data stores and physical items (such as building doors and equipment) that are within the organisation. Auditing, the third process in access control, creates a user-activity trail. Administrators can analyse the audit trail and identify access anomalies (Bigelow, 2008).

Furthermore, business owners and managers are constantly identifying areas of risk and taking steps to mitigate that risk. In an IT environment, risk takes the form of access. An organization may possess a wealth of resources, but those resources are not protected by the organisation (Bigelow, 2008). If the resources are damaged by unknown users it means that the access control system used in such an organisation is not effective. Hence, there is need for an improvement in the access control policy used by such an organisation which will assist to examine if all activities that took place in the access control system complement the initial plan or the set purpose of the system. Audit control is helpful; it has the ability to identify misconduct performed previously; examine the way users' act when using the access control system; identify actions that violated the system; and guide or advise in terms of how to prevent misconduct and violation of the system.

In addition, Bigelow (2008) identified that auditing is a measures that can be used to determine whether the access control system is effective or not effective. An audit control is based on empirical analysis of all the requirements and users' actions in the system. In order to perform auditing, all records of the users' actions are needed together with what was required to be performed according to the initial plan. Possible errors in the security of the access control system can be identified during the auditing process. Auditing can also recognise if users abuse their privileges of gaining access to the organisation. Auditing takes place to verify if the system achieves its purpose; if not the access control policy, plan or implementation should be reviewed in order to complement the objective of the organisation. In case there is a need to change policy, plan or the way the system is utilised, proper change management principles need to be applied.

In addition, effective security starts with understanding the principles involved in an organisation. Because of its universal applicability to security, access control is one of the most important security concepts to understand. Employees must be aware of the security standards set for an organisation. Hans (2014) indicated that property and asset owners or managers desire a safety solution that suits their objectives; in that regard risk to such cannot be tolerated. Management of organisations can benefit tremendously from the continuously growing technology by implementing new IT solutions using change management principles. This implies that management can decide to change the access control policy if it does not secure or protect the organisation’s property.

Iconic (2016) indicated that an integrated and structured security risk management plan is essential for all buildings, both business-related and residential, where there are multiple uses or occupancy. An effective and professionally installed access control system must form part of such a management plan. He also highlighted that modern technology has led to different designs and manufacture of access control system as such care must be taken to ensure that these new technologies and applications are suitable and capable for the intended use. Taylor (2017) argued that for effective access control to take place in an organisation there is a need to balance effectiveness with operational efficiency, meaning you cannot shut down operations in the name of security. Services need to be provided to constituents but not at the cost of security. Revenues need to be collected, car transfers need to be distributed, home improvement inspections need to be done, and police officers need to continue to ensure public safety, and so on. Business still needs to go on, but at the same time, you need to have adequate security measures in place. As such, there is need for organisations to implement better ways of improving access control management.

Carrtegra (2015) highlighted ways managers in an organisation can improve the access control management in the organisation. These include:

- Ensuring that there is support from senior management and board and there is a top-down drive to establish and communication policies with regard to IT security and access management. The top-down drive sets the direction, goals, and tone of the IT security and access policies and holds users accountable for any action on any of the systems and/or applications involved.
- Ensuring that there are defined processes for identifying new users and recording, approving and maintaining access rights; in determining this process, the user access right should be in line with the business needs, the access right should be requested and approved by the user management.
- Establishing a method for authenticating and authorizing users to establish responsibility and enforce access rights in line with sensitivity of information and functional application requirements and infrastructure components, and in compliance with applicable laws;

- Ensuring that users and their activities on the system can be uniquely identifiable; this can be done by ensuring that shared user accounts are not used; shared accounts are used more often for vendor's access, temporary accounts, and administrator's account and they are extremely high risk in an organisation;
- Ensuring that there is a process in place to periodically review user access by user management and system/data owners

From the above literature, it is evident that there are various access control systems that could be used in an organisation. Effective use of these access control systems in an organisation will enable them to secure their properties and also protect the safety of the staff.

Organisations encounter various challenges in order to ensure that the access control system used in the organisation is effective. The next section will review the challenges that are faced by organisations in using an access control system.

2.9 CHALLENGES FACED BY ORGANISATIONS IN IMPLEMENTATION OF ACCESS CONTROL SYSTEM

According to Brandewie (2009), there are constant reminders of the threats to our institutions and the vulnerabilities that are raised when a strong programme of identity management has not been implemented in the enterprise. Various challenges on how to implement these access control systems continues to prevail. These challenges include:

- Lack of standardization where organizations are locked into technologies that have failed to keep pace; worst of all, there are too many instances of using organization credentials as flash passes for facility access;
- Dynamic response to changing threat levels is another essential challenge; this involves a prepared plan of who needs access during a period of heightened threat and how the authentication and access plan should change to raise the security of the access;
- Managing access privilege; a new generation of smart badge readers is emerging who are essentially mobile smart card readers that have been paired with physical access radio frequency identification (RFID) technology;

These readers allow the employee as they approach the access control barriers to enter his/her PIN code, which opens the smart card credential; organisations who have these types of system are struggling on how to manage it; visitors to the organisation are also a challenge in respect of managing their entries and exits;

- Password problems also present a challenge in organisations; employees must remember an increasing number of passwords for applications that may cross domains and use numerous different authentication and attribute-sharing standards and protocols; user frustration can mount when an employee spends more and more time managing the resulting lists of passwords which, for some applications, may require changing after a specific period, plus, when employees have trouble with their passwords, they most often contact IT staff for help, which can quickly and repeatedly drain important resources (White Paper, 2016).

Therefore organisations can ensure security by deploying solutions with strong multifactor authentication, while eliminating user frustration by delivering seamless access to cloud-based information. The next section will specifically review the manner in which access control systems are used in HEIs.

2.10 ACCESS CONTROL MANAGEMENT AT HIGHER EDUCATION INSTITUTIONS

We are living in a period where communities practise their right of demanding what is due to them through striking. With reference to South African universities, in 2015 there was a fees-must-fall strike and other in-sourced employees, in particular cleaners from some South African universities, joined the strike demanding to be employed permanently by the institutions. Some of the strikes were legal while others were not. For the duration of those strikes, the property of other institutions was burnt down, made possible by poor monitoring of access at entry points. During strikes the safety of all those on campus is compromised, if the access control system is not sufficiently credible. The safety of workers, students and genuine visitors is a crucial matter for the university management (SABC, 2016).

Hans (2014) conducted a study examining the access and exit control system of vehicles utilised by the Tshwane University of Technology (TUT). During the study TUT was using two methods; staff members and students were swiping cards at the gate, while visitors were registering their details in the logbook. According to Hans (2014), these systems had the possibility of conveying a number of risks to the university. There is the chance of losing cards or they can be stolen then used to exit campus with stolen goods like cars and cell phones. With the logbook, visitors can produce a false identity with the intention of performing illegal activities on campus. Hans (2014) affirms that illegal activities took place at other universities in South Africa using similar systems and TUT needed to avoid such activities.

Access control systems using a card and manual logbook are not efficient since they cannot avoid other risks (Hans, 2014). The implementation of a fingerprint biometric clocking system was proposed to avoid risks that come with using a manual logbook, student and staff cards to access and exit TUT campus (Hans, 2014). The reason behind proposing a fingerprint biometric clocking system is the uniqueness of the features utilised to validate access; no staff, student or visitor can lose and forget the feature that is used to gain access. Moreover, the feature cannot be stolen. The fingerprint biometric access control system has been tested to be effective and efficient in other environments (Hans, 2014).

Structural matters, e.g. the magnitude of the institution and the level of assembled IT services and related policies and actions have an effect on the final access control system outcome (May et al., 2006). A systematic approach is necessary when developing and implementing access control systems for the purpose of simplicity. The difference from one institution to the other is the culture and the various functioning systems deployed (May et al., 2006).

From society’s point of view, HEIs are to a certain degree reflected through actions, tradition and processes (May et al., 2006). This also incorporates the degree to which ICT is encouraged and reflected in the security customs of the HEI. The access control method that does well in the security space has the potential to improve the operational standard. The values and standards of HEIs eventually reflect the values of the society (May et al., 2006).

Institutions have to develop a tradition of security in all components and acknowledge the necessity of IT security and information communication and technology (May et al., 2006). The ICT space is constantly advancing the operations of organisations and bringing reliability and innovation to the business environment. Nowadays, technology underpins many areas in an organisation and access control is no exception.

2.11 SUMMARY OF THE CHAPTER

In this chapter, the review of relevant literatures in relation to the various access control systems used in an organisation was made. The level of effectiveness of the access control system, the relevance of the access control system, various access control systems used in organisations and the challenges of the implementation of the access control system in an organisation, as well as in higher education and how it could be managed at an HEI, were reviewed. From the literature, it can be deduced that there are various access control systems that can be used in an organisation but organisation experience difficulties in successfully implementing these access control systems.

The next chapter will present the research design and methodology that will be used to investigate the effectiveness of access control at SPU.

CHAPTER THREE
RESEARCH METHODOLOGY

3.1 INTRODUCTION

In the previous chapter, relevant literature was reviewed with respect to the study under review. In this chapter, the research design and methodology will be identified and discussed. This chapter would enable the researcher to determine the procedures by which the data for this study will be collected.

3.2 RESEARCH PROCEDURES

The research proceeded along the following steps as illustrated in Figure 3.1.

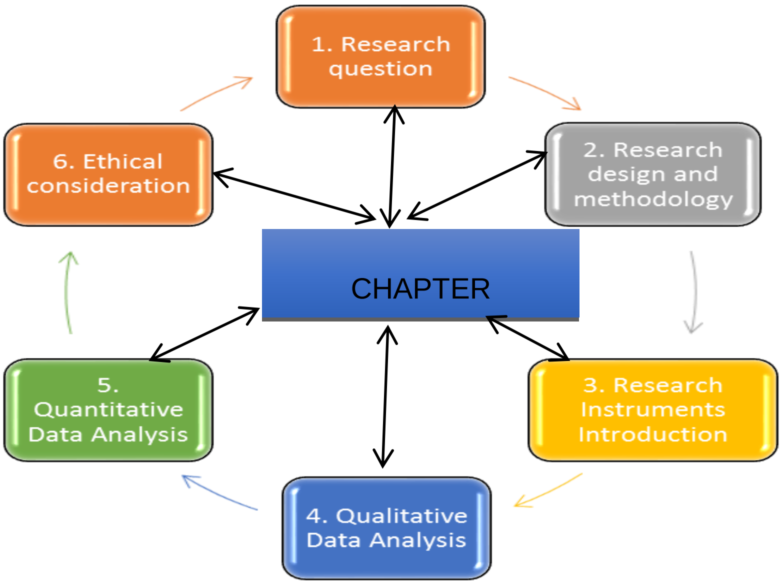

1. Research question
2. Research design and methodology
3. Research Instruments Introduction
4. Qualitative Data Analysis
5. Quantitative Data Analysis
6. Ethical consideration
CHAPTER

Figure 3.1 Chapter procedures

3.3 RESEARCH QUESTIONS

As noted in Chapter One, the present study seeks to answer these research questions:

- What is the access control policy management used at SPU?
- What are the challenges faced by SPU in access control management?
- What are the perceptions of students and management on the access control management used at SPU?
- How effective is the access control policy management used at SPU?

- In what way(s) can the access control management be improved at the institution?

3.4 RESEARCH DESIGN

According to Maree (2010), research design is a strategy that is typically based on a philosophical assumption which helps in the selection of participants (qualitative) or respondents (quantitative), data collection procedures or statistical techniques to be used for the study and the analysis to be done. According to Creswell (2014), a researcher's philosophical assumption, design and methods all contribute to a research approach which can be quantitative, qualitative or a mixed methods approach.

Mixed methods research is a research design with philosophical assumptions as well as methods of inquiry. As a methodology, it involves philosophical assumptions that guide the direction of the collection and analysis of data and the mixture of qualitative and quantitative data in a single study or series of studies. Its central premise is that the use of quantitative and qualitative approaches in combination provides a better understanding of research problems (Creswell, 2013).

Quantitative research aims at testing a research hypothesis and involves analysis of numerical data. The interest of this research approach was to understand how a particular phenomenon might be generalised to a larger population (Allen, Titwork & Hunt, 2009).

A qualitative research approach, on the other hand, has to do with the collection of extensive narrative data (non-numerical data) on many variables over an extended period of time in a naturalistic setting. The rationale for using the two methods is for one method to complement the deficiency of the other. In general, mixed methods research represents research that involves collecting, analysing, and interpreting quantitative and qualitative data in a single study or in a series of studies that investigate the same underlying phenomenon.

For this study, a mixed method research design will be used. Mixed method research is the combination of both qualitative and quantitative research. The mixed method was chosen for this study in order for the researcher to gain in-breadth and in-depth understanding and corroboration, while offsetting the weaknesses inherent in using each approach by itself. One of the most advantageous characteristics of conducting mixed methods research is the possibility of triangulation, i.e. the use of several means (methods, data sources and researchers) to examine the same phenomenon.

Table 3.1: Interaction between mixed, qualitative and quantitative research design

Quantitative	Mixed	Qualitative
Pre-determined method	Both pre-determined and emerging method	Emerging method
Instrument based question	Both open and closed ended questions	Open ended questions
Performance data, attitude data, observational data, and census data	Multiple forms of data drawing on all possibilities	Interview data, observation data, document data, and audio-visual data
Statistical analysis	Statistical and text analysis	Text and image analysis
Statistical interpretation	Across databases interpretation	Themes, patterns interpretation

Adapted from Creswell (2013:1)

3.4.1 Alignment of research aim, questions and data collection instruments

It is important to align the research aim for this study with the data collection instrument in order to present a clearer view on how data will be collected in relation to the research design used. Table 3.2 presents the alignment. Only instruments suitable for achieving the research aims will be used for data collection and the presentation and analysis of results (chapter four) would be done according to the instruments used.

Table 3.2: Alignment of research aims, questions, and data collection instruments

Research aims	Research questions	Instruments
x **Investigate the access control policy management used in SPU**	What is the access control policy management used at SPU?	Interviews
x **Examine the**	What are the challenges	Interviews

challenges faced by SPU in access control management	faced by SPU in access control management?	
x **Examine the perceptions of students and management on the access control management used at SPU**	What are the perceptions of students and management on the access control management used at SPU?	Questionnaires and interviews
x **Investigate the effectiveness of the access control policy management used at SPU**	How effective is the access control policy management used at SPU?	Questionnaires and interviews
x **Investigate way(s) access control management can be improved at the institution**	In what way(s) can access control management be improved at the institution?	Interviews

Adapted from (Creswell & Plano Clark, 2007:112)

3.5 RESEARCH METHODOLOGY

Methodology is an indispensable part of a research project; this section gives the information that is used to measure the validity of the research (Kallet, 2004). The importance of research methodology is to guide and determine how to approach research questions. It also pays attention to the research process and the conclusion that the researcher reaches. It is important for researchers to choose a method that is suitable to derive optimum answers to the research questions and achieve the research objective.

The design chosen is the exploratory sequential mixed method, which covered two phases. The empirical research started with the qualitative method then was followed by the quantitative method. An exploratory sequential mixed methods approach is the reverse sequence from the explanatory sequential design. This method was chosen in order to enable the researcher to first begin with a qualitative research phase and explores the views of participants. The data are then analyzed, and the information used to build into a second, quantitative phase. The qualitative phase may be used to build an instrument that best fits the sample under study, to identify appropriate instruments to use in the follow-up quantitative phase, or to specify variables that need to go into a follow-up quantitative study. Particular challenges to this design reside in focusing on the appropriate qualitative findings to use and the sample selection for both phases of research (Creswell, 2013).

3.5.1 Population and site selection

A population can be seen as the total number of people inhabiting a country or a city. The population for quantitative part of the study is all students at SPU. There are 135 students at SPU and these form the total population for the study. As indicated earlier, SPU is a new university with a low number of students. The university is still growing and currently operated with five faculties (schools) with a low number of students in each faculty.

A site is described as a group of individuals in a setting or a population who possess specific characteristics and from which the participants are drawn to determine the parameters (Creswell & Plano Clark, 2007:112). Maree (2007:34) points out that a research site must be suitable and feasible in the section chosen for a qualitative study. There are four schools iat SPU (School of Education, School of Natural Science, School of Economics and Management science, and School of Humanities). The students in these schools and the security managers are the target population for this study.

3.5.2 Sampling and participant selection

The reason behind sampling is to determine the population category and size that will used to participate in the study. That population (users) will provide their views and experience regarding the effectiveness of the current access control of SPU. In order to capture those views and experience of the targeted population, questionnaires will be developed by the researcher and completed by participants; one-on-one interviews will also take place. At times it is a challenge to gather data from all the targeted individuals in a population; some of the reasons that hamper the success of that exercise are limited time and cost to perform the data collection activity. Hence it is simple and smart to collect data from a sample instead of the entire population.

To determine whether the access control system of the SPU is effective or not will depend on the information obtained from the population sample. It is indispensable that all the population segments (staff, students, visitors) within the sample are represented in the population sample. That will put more weight on the analysis to gauge if the parties in the sample differ or have similar views about the access control system. It is not legally binding to respond to questionnaires and interviews although participants are encouraged to complete the questionnaire and respond to questions. This would increase the credibility of the analysis.

The sampling method is chosen based on the specific verdict of the researcher. There is non-probability sampling and probability sampling; probability sampling includes random selection while non-probability sampling eliminates random sampling. Even if non-probability samples do not eliminate random sampling, it still relies on the basis of probability theory. In this study non-probability sampling will be used. Other elements of analysis do not get an opportunity to be included in the sample when using non-probability sampling (Welman et al., 2005). Robinson (2014:25-41) stated that sampling involves selecting research respondents from a population who will answer the research questions. Sampling is the method utilised to choose the components and the quantity of the population for an investigation (Creswell et al., 2007). Sample size on the other hand is the quantity of observations to be collected that will be utilised for generating analysis in the research (Welman et al., 2005).

In this paper the sample size will be a specified number of individuals who are responsible to oversee the effectiveness of the access control and the users. Their response will be formulated in the formation of the determinants of whether the access control system is effective or not. For the purpose of the quantitative part of this study, the researcher made use of a census survey whereby all students from the four schools at SPU were used as respondents for the study.

Table 3.3: Number of students in each school at SPU

Schools	**Number of students**	**Number of students selected**
School of Education	800	40
School of Natural Sciences	352	35
School of Economics and Management Science	1022	45
School of Humanities	208	15
Total	2382	135

Not all students were used for the study. The researcher employed a simple random sampling method to select 135 respondents for the quantitative research. Simple random sampling is the basic sampling technique where the researcher selects a group of subjects (a sample) for study from a larger group (a population) (Creswell, 2009). This means that selected students from each school at SPU were chosen by chance and had an equal chance of being selected.

The participants that would be used in the qualitative part of the study are the security officers. These include the security manager and staff in the security department. There are two security managers and seven staff members. Hence a total number of nine participants would be interviewed in the qualitative part of the study. These participants were chosen by the researcher because they serve as key informants to the study under review.

The chosen research methods and techniques simply imply that the investigation outcome will be descriptive research; individuals' own opinions (uttered or written). This means that people will provide their actual experiences. The results of this investigation, which is based on qualitative research, will not be established from statistical principles or processes. The purpose of the questionnaire will assist in finding the actual experience of the targeted population groups regarding the access control system of SPU.

3.5.3 Data collection

The researcher adopted a structured closed ended questionnaire as the instrument of data collection in the quantitative data collection. The questionnaires used for the study were structured in such a way to enable the collection of accurate facts on the respondents’ opinion concerning access control management in SPU.

Questionnaires were used for the following advantages, outlined by Popper (2004) and Ackroyd and Hughes (2010):

- It is practical.
- Large amounts of information can be collected from a large number of people in a short period of time and in a relatively cost-effective way.
- It can be carried out by the researcher or by any number of people with limited effect on its validity and reliability.
- The results can usually be quickly and easily quantified by either a researcher or through the use of a software package.
- It can be analysed more 'scientifically' and objectively than other forms of research.
- When data has been quantified, it can be used to compare and contrast other research and may be used to measure change.
- Positivists believe that quantitative data can be used to create new theories and /or test existing hypotheses.

An interview schedule (see Addendum A) was developed for collecting data during semi-structured interviews for the qualitative data collection. According to McMillan and Schumacher (2006), an interview is made up of open-ended questions that allow respondents to express themselves and give their individual views and meaning to a phenomenon. Barbour (2008:114) also affirmed that an interview enables the researcher to obtain relevant, valuable and analytically rich data. A respondent interview was viewed as best approach because it enables the researcher a closer interaction with the respondent for in-depth understanding on the topic. Participants were interviewed during lunch time in order to avoid misusing the company's resources. This enabled the researcher to also read the interview actions when answering and get more clarity on the underlying issue. Interviews were used by the researcher for the following reasons:

- It allows the researcher easy correction of spoken responses made by the participant ;
- It also helps in the selection of suitable candidates for the study, namely staff of the security department;
- It helps in the collection of sufficient information;
- Interviews are less costly than other ways of communication; ithey are simple, convenient, and provide a prompt response.

The data gathered through interviews with the security staff and managers will enable participants to provide their views while simultaneously their reactions to using the access control system will also be observed. This will improve the credibility of the results since more than one data collection method will be used. Telephonic and email interviews will also be done for staff who could not attend the interviews.

3.5.4 Data analysis

Data needs to be captured into a program that is capable of transforming it to provide meaningful information that can be used for decision-making; the computer program to be used is Microsoft Excel. For the quantitative data collected, a descriptive data analysis will be conducted. The questionnaire will be populated into Microsoft Excel. The populated data will be presented in a simplified manner by developing tables and graphs that will be used to analyse the output, while the data collected from the interview will be presented in themes and categories. The themes will be the research objectives for this study and the categories will be the responses coded from the participants. The purpose of doing this is to enable the researcher to have a clearer view of the participants' and respondents' responses and also be able to discuss their responses in the next chapter.

3.6 ETHICAL CONSIDERATIONS

Ethics are norms and standard of how to behave or act, and guide us to act and behave in an acceptable manner (Cooper et al., 2011). In the process of analysing the effectiveness of access control at SPU it is imperative to be mindful of the ethics related to all aspects that will be addressed. One of these is to acknowledge the views of all those who participate in the research.

When drafting the questionnaires, the researcher will acknowledge and ensure the privacy of the respondent as this is of the utmost importance. The details discussed in this paper will be presented in a manner that will not impair the image of the university's staff and students, or visitors to SPU.

To ensure proper ethical consideration, the researcher is required to obtain a letter from the higher committee in the School of Business (see Annexure B) that would enable the researcher to gain access to SPU. The researcher has to acknowledge and maintain the confidentiality of data provided by respondents by not disclosing information to any party who is not in collaboration with the study and preserve the participants' anonymity. The data collected will be used only for the purpose of achieving the objective of this research. The respondents in this research will not be forced to answer questions and participation will be voluntary.

According to Lekganyane (2011), terms as trustworthiness, credibility, conformability, consistency or dependability are key words in qualitative research; dependability in qualitative research closely matches the notion of reliability. Maree (2010:299) stated that trustworthiness is the ability of the researcher to persuade the audience that the research work is worth paying attention to. Lincoln and Cuba (in Marshall & Rossman, 2011), explained that in attaining research trustworthiness, some distinct procedures must be maintained, e.g. prolong engagement, meaning that the researcher should be in the setting for a long period of time; member checking which urges researchers to share data and interpretation with the participants; triangulation by gathering data from multiple sources; and peer debriefing, which requires the discussion of emergent findings with critical friends to ensure that the analyses are grounded in the data.

To ensure trustworthiness, the researcher gave a copy of the interview guide and the questionnaire before the scheduled interview for each participant and respondent to study. He asked the participants to feel free to contribute or share any other relevant information during the interview. This allowed the participants an opportunity to speak freely. Cresswell (2005) also stated that throughout the process of data collection and analysis, the researcher needs to ensure that his/her findings and interpretations are accurate.

3.7 DEMARCATIONS OF THE RESEARCH

One critical possible demarcation to this study is time. The availability of the security staff might be a possible limitation on receiving responses from them given their daily eventful management activities. There is also a chance that students might procrastinate to fill the questionnaire but that will depend on their daily class schedules. As a result, more clarity will be presented to everyone emphasising the importance of completing the questionnaire.

3.8 SUMMARY OF THE CHAPTER

The importance of the methodology chapter is that it provides information used to measure the validity of the research (method and sampling technique); it guides and determines how to approach research questions. It also pays attention to the research process and the conclusion that the researcher reaches. Both the qualitative and the quantitative approach were identified to perform the analysis. The next chapter will present and discuss the findings made from the study.

CHAPTER FOUR
ANALYSIS AND PRESENTATION OF FINDINGS

4.1 INTRODUCTION

The previous chapter presented the research approach and methodology adopted, and the current chapter presents the data analysis for both the qualitative and quantitative part of the study with the presentation of findings. The qualitative findings are presented according to the themes as they emerged from the study in order to reflect the participants' direct meanings while the quantitative findings are presented in the form of tables and figures.

The study employed the exploratory sequential design, which first presents the qualitative findings. An analysis of the quantitative findings was made in order to be able to quantitatively confirm participants' response from the qualitative data collected.

4.2 QUALITATIVE DATA PRESENTATION AND DISCUSSIONS

An interview was conducted with the security managers and the staff members who are the selected participants for the qualitative phase of the study. Table 4.1 presents the pseudonyms used to represent the participants for easy identification.

4.2.1 Research questions

The following research questions were asked in this study:

- What is the access control policy management used at SPU?
- What are the challenges faced by SPU in access control management?
- What are the perceptions of students and management on the access control management used at SPU?
- How effective is the access control policy management used at SPU?
- In what way(s) can the access control management be improved at institutions?

4.3 PSEUDONYMS OF PARTICIPANTS

Table 4.1: Pseudonyms

Participants	**Pseudonyms**
1. Security manager	SM
2. Staff members	Sn

According to Rossman and Rallis (2012:262), qualitative researchers generate data from different participants using different techniques. They then transcribe the collected data, removing the junk thereby reducing the data and carry out the coding process in order to arrive at the participants' authentic meaning with regard to the study. However, the coding process of this study was done using the response of the entire staff of security officers (security manager and staff managers) who are represented with alphabetical characters: SM for security managers and Sn for staff members for accurate recognition. There are two senior managers in the study represented as SM01 and SM02 whereas the staff members bear the designation Sn01 to Sn07 respectively.

4.4 THEMES AND CATEGORIES IDENTIFIED IN THE STUDY

Table 4.2: Themes and categories

Themes	Categories
Understanding on access control	• Procedures to gain entrance • Control of regulation of access
Possible access control used at SPU	• Limited access control • Card control system • Rules of management
Challenges faced by university in managing access control	• Protest and strike • Loss of cards • More presentation of cards • Access from unregistered students
Improved security	• Effective • More security
Effectiveness of access control policy used	• Check the response and create a general category
Ways of improving access control management	• Increase security visibility • Use of biometric system • Proper gates and fencing • Fingerprint system • Enforce disciplinary procedures

To better understand the participants' responses as regard to the study, the presentation and discussion of the research findings reflect the research questions but are structured according to the generated themes and categories that emerged from the response of the security managers and staff members.

4.4.1 Access control policy management used at SPU

4.4.1.1Understanding on access control

In order to assess the level of understanding of the access control policy management used at SPU, the researcher asked the participants a number of questions on their understanding of the policy before contextualising the question to the access control policy used at SPU. The response from SM01 follows:

> They are procedures undertaken for one to gain entrance into the university premises with the advancement in technology and the need to safe guard the university environments on the basis of controlling the in and out movement of students, staff, non-academic staff and even non students and non-staff, university managements are using access control system to check mate the movements (SMO1).

Khan (2012) supported the statement of **SM01** by saying that access control systems are becoming more sophisticated because of new innovative developments in the field of access control. Hu et al. (2006) agree that sufficient safety of information, assets and people is an essential task for management in organizations hence the need for an access control system. Teh et al. (2013) argued that the management of access control and its policies in an organisation cannot be flawless as a result of the laws and policy by people within and outside the organisation. It can therefore be deduced that proper control of the policy of access control in an organisation can improve the management thereof. **SM02** indicated that

> Access control refers to the access you have to a place, such as a university. There is no way all manner of persons can be allowed access into a university or organisation the same; it will jeopardize the security of the institution or organisation hence access control system is very important (SM02).

In support of the participants' answers, Hu et al. (2006) maintained that access control could also be defined as a mechanism that permits or prohibits a person the right of entry to a specific location. One of the functions of access control is to trace or record the number of people going in and out and to know their motive and their whereabouts in the jurisdiction of the organisation. Those records can be used as data trails when performing audits or monitoring compliance. Participant **Sn03** maintained that access control entails

> Controlling and regulating the access of people to a specific area, however, these people are those legally granted permission to that area but the use of access control helps the organizational mangers to still be in control of the area, like in the university, controlling the entrance and exit of people or students will enable the school management to be keeping the appropriate data and statistics of the people (Sn03).

Adding to this, Hu et al. (2006) elaborated by arguing that the access control system must determine who can enter, when and where; the system is utilized in order to improve safety and allow people with rights to gain access to do so. Patil et al. (2012) agree that there should be a policy indicating who may access or may not access the organisation. It may be inferred that this strict policy can help to control the access of people within and out of an organisation. **Sn08** is of the opinion that

> Access control is a security system that allows an authority person to control access to certain areas of a building. It involves a vestibule where people enter and do whatever is necessary to get into the controlled area. Security of a place should be imperative to management; hence the need for access control (Sn08).

Sn01 further added that among the regulations of the access policy used in SPU is

> **...** limiting access to people with student or staff cards and visitors as this allows the facility users limited access to certain places in the university which helps in taking control of the university facilities and control the movement of people(Sn01).

An access control model plays a role in bridging the gap between policy and mechanism. Hu et al. (2006) further explained that one of the policies related to access control system policy is the security policy which must enforced through a system; the security policy determines limitations. Maximum freedom to access every entry at the organisation could result in unauthorised entrance (Hu et al., 2006).

These findings are in line with the system theory on access control used in this study, which emphasises the need for adopting proper security management in order to ensure that the organisation as a system is secured (Cavusoglu et al., 2012).

4.4.1.2 Possible access control used at SOL

Sn03 went further to say that

> ... the university uses a card system to control access. The students, staff and non-academic staff have to swipe their cards before they can have access to the university (Sn03).

To this end, Teh et al. (2013) expanded by stating that there are different types of access control systems that can be deployed in order to manage access of individuals. Those access controls are either manual access control or electronic. Manual access control systems are in the form of physical keys and a logbook register while the electronic access control systems are keypad, smart card and biometric access control system. However, the manual access control system, to a certain degree, has limited capability to cover the entire purpose.

On the contrary, findings from participants showed disagreement. For example, **Sn04** is of the opinion that the university has no formal access policy yet:

> To my best understanding, we are using rules agreed with management to control access; the rules are made by the management (Sn07).

Sn07 went further to reject the opinion of **Sn04** stating that

> Access management is control through an IT card system. People who don't have cards have to sign in at the security desk. The signing is being monitored by the security personnel which goes a long way in monitoring the in and out movement of the students, staff, non-academic staff or visitors. Any of the formal facility users in the university that misplaces his or her card or forgets to come to campus with it is mandated to report to the security before the person can be allowed into the campus (Sn07).

Hu et al. (2006) supported the above statement by saying that one of the policies related to the access control system policy is the security policy which must enforced through a system and the security policy determines limitations. Furthermore, maximum freedom to access at every entry of the organisation can result in unauthorised entrance (Hu et al., 2006).

SM02 maintained that

> The major control policy in the university is centred on the use of access cards by all students, staff and non-academic staff, so the use of a student card helps to keep the data of all the individuals (SM02).

The study by Patil el al. (2012) agrees with the findings from the participants by indicating that the policy regulates the users' access information and the access can be given to the user based on his or her identification.

From the findings, it is evident that access control at SPU is controlled by policies and the use of cards and passwords, even though Brandewiee (2009) argued that the password problem is a challenge in an organisation which should be dealt with. As such, the next session will discuss the challenges faced by SPU in access control management.

4.4.2 Challenges faced by SPU in access control management

At this point, the researcher asked the participants about the challenges faced by the university in managing the access control system for a proper understanding of the subject under study. According to **Sn01**

> The university is organised and always endeavours to keep the system working by providing the necessary technology and equipment which fosters the effective management of the school. The access card system has been helping in controlling the in and out movement of the people on the campus and has restricted the unauthorised use of facilities by the students so to me, I am not aware of any challenges faced by the university in managing access control (Sn01).

Sn02 is of the opinion that striking is among the challenges faced by the university in managing access control:

> During the time of any protest, it puts lots of pressure on the school management. Controlling the students becomes a huge problem.

The participant strongly posits that striking is a serious challenge to South African universities because students usually capitalise on destroying university property which incurs unnecessary expense to the government. In addition to this, according to the SABC (2016) with reference to South African universities, in 2015 there was the Fees-must-fall strike joined by other in-sourced employees because cleaners from some South African universities joined the strike demanding to be employed permanently by the institutions. Some of the strikes were legal, others were not. For the duration of those strikes, properties of other institutions were burnt down; made possible by poor monitoring of access at entry points. During a strike the safety of all those on campus is compromised if the access control system is not credible. The safety of workers, students and genuine visitors is a crucial matter for the university management.

Furthermore, **Sn03** maintained that

> Despite the positive side of access control system in the universities, the challenges are still numerous such as losing the access card by an individual which can be picked up by an unauthorised person thereby using it to perpetuate crimes in the school or the challenges of malfunctioning of the card reader at a door which affects the movement of the people (Sn03).

Hans (2014), in agreement with this participant, posits that these systems had the possibility of conveying a number of risks to a university. There is the chance of losing a card or cards can be stolen then used to exit campus with stolen goods like cars and cell phones. With the logbook, visitors can produce false identity with an intention of performing illegal activities in campus. Hans (2014) agrees that illegal activities have taken place at other universities using similar systems in South Africa (RSA) and TUT needs to avoid such activities.

SM01 also maintained that

> Our campus is an open campus with many public spaces. Turnstiles are sometimes bypassed and not effective. Students are sometimes not cooperative.

When a campus or an organisation is in such shape, maintaining proper security of the place becomes most challenging; students tend to manoeuvre the existing facilities to suit themselves which adds a huge burden on the management. IN addition, owing to the fact that students or facility users are made up of people from different backgrounds, it becomes more difficult to deal with and a lack of cooperation increases the challenges on the management. There is a need to also find out the perception of students and management on the access control management used in SPU. The next section will present these findings.

4.4.3 Perceptions of students and management on access control management at SPU

4.4.3.1 Improved security

To obtain further understanding of the study, participants were asked their opinion of the access control policies used by the university as this would help the researcher to gain more insight into their perceptions. Participants gave their thoughts and opinion on the question. For instance, **SM01** stated that the access control system used by the university was effective but its effectiveness was regularly hampered by the unruly behaviour of some service users, e.g. an individual would give his or her access to a friend and the person would misuse it.

Sn02 argues that

> Access control management used in SPU is really effective with good measures because the in and out movement of people is controlled. In the time past, the university struggled to control the movement of people in and out but presently, things are much better. The access control system has taken security to a higher better level and the security personnel around the gates are doing much better (Sn02).

According to Khan (2012), access control systems are becoming more sophisticated because of developments in the field of access control. Hu et al. (2006) added that sufficient safety of information, assets, and people, is an essential task for management in every organisation. Brandewie (2009) argued that there is a lack of standardization and organisations are trapped into technologies and securities that have failed. Furthermore, the access control system must determine who can enter, when and where. The system is established in order to improve safety and allow people with rights to gain access to do so. It is important for the access control system to record the name of the individual, contact details, time an individual entered and exited the premises. That information helps management to make informed decisions.

The viewpoint of **Sn03** is:

> I don't think an access control system is that necessary. This is a university and to me it should be an open access area for people to come in and go without the security personnel or anyone to start questioning the individual. Again, access control system is hard to handle owing to the fact that the university is open (Sn03).

However, contrary to the beliefs of this participant, the researcher believes that a proper access control system in organisations is indispensable and is meant to make users accountable for their acts since they can be monitored. Moreover, it prevents an individual from abusing the system. The purpose of access control is to determine the allowed entry or activity for a genuine user. To a certain degree, the safety of all stakeholders (employees and other stakeholders), assets and information in the company depends on the system.

SM02 argued that

> Further expanded, the access control system used by the university has been very helpful to us. Since the university started the use of access cards to control the in and out movement of people into the university, there has been a better control as an outsider doesn't come in to misuse the university facilities and the service user are becoming more comported. The access control system is making management of an organisation much better since the database of all the facility users take records of whenever they swipe at the gate which always helps in retrieving information in time of problems (SM02).

Sn04 is in agreement with **SM02** adding that the "access control system makes the university more secured and it works cooperatively as a system".

In support of these findings, Hu et al. (2006) reported that a properly regulated access control system can classify sharing of information according to the rank of the user but when that mechanism does not exist sharing of information can be unmanageable. For example, a worker who is responsible to administer the server room facilities must be granted the privilege to access the server room in order to perform his or her enforced duties within that area and have limited access if not to access other areas in the company like the financial archive space. The access control system helps organisations make every individual involved in a specific operation of the business accountable. Also working together as a system in an organisation in order to enhance the control of access in an organisation can be viewed in accordance with the systems theory on access control used in this study. According to Conklin and Dietrich (2008), systems theory enables an organisation to work as a team and devise strategies that will help in managing the movement of people within and outside the organisation.

Additionally, the access control system advocates for segregation of duties because if it regulated appropriately, the limitation of access will make it possible for every individual to focus on the activity that he or she must perform. One example can be in the finance unit where one-person access to collect revenue from clients and the other person can be allowed to bank the money while the third will gain authority for reconciling financial records. A well-managed access control system has the ability to reduce irregular and wasteful activities that cost the organisation a considerable amount of money. The organisation needs to craft a hierarchy that determines authorisation of individuals' access to the entry points of the organisation. Having this in mind, the next section presents the findings made on the effectiveness of the access control system at SPU.

4.4.4 Effectiveness of access control policy management at SPU

4.4.4.1 Effectiveness of access control policy

In order to answer the research question on the effectiveness of the access control policy management used by SPU, participants were given the time to understand the question; their opinions follow.

SM01 responded:

> The access control policy management used in SPU has so far been effective over these years because there hasn't been lot of reported cases of ineffectiveness as regard to the university's access control policy. Security wise, the university is really trying because truants don't have access to the university vicinity because of the access control policy in use and the databases of all the facility users are taken record of each moment the individual comes or try to use any of the faculties (SM01).

In this connection, Sandhu et al. (1996) supported these findings by reporting that the access control policy and the security policy are put into effect by the access control system that is made possible by the IT security. Furthermore, **SM01** added that "the policies are not too stringent because it is to the security of the entire facility user".

Sn03 is also in affirmation with **SM01** but added "The policies are sometimes tampered with, for instance when a student loses his or her access card or gives it to a friend to use".

SM02 has a different answer to the question by saying

> To my own opinion, the access control policy management used in the university is not effective because the university is still new, hence most of our implementation methods are on trial and error; we are still learning (SM02).

Another participant, **Sn04,** stated

> The access control policy management used by SPU is effective but the implementation is always difficult. For instance, management most times fails to take pragmatic actions toward ensuring the implementation of laid down policies and punishment of defaulters (Sn04).

Hans (2014) concurs that an access control system, such as cards and manual logbook, are not sufficient since they cannot avoid other risks. Nigam et al. (2015) suggested the use of a biometric access control system. Biometrics is an essential element of identity science and commonly used in the IT security field for the purpose of recognizing people. The first biometric used was called soft biometrics established by Bertillon in the nineteenth century (Nixon et al., 2015). Later in the early twentieth century a biometric system using fingerprints was established. From there more studies revolving around biometrics were conducted (Lumini et al., 2016). Innovation played a critical role in advancing the field of biometric access control; more than one feature of a human body can be used to validate access (Nixon et al., 2015).

Sn05 and **Sn06** are in agreement on the effectiveness of access control management used in SPU stating that "The policies help in keeping the database of the facilities serving the users". In support of the participants, Hu et al. (2006) went further to define access control system as a mechanism that can permit or prohibit a person the right of entry to specific location. One of the functions of access control is to trace or record the number of people going in and out and to know their motive and their whereabouts in the jurisdiction of the organization. Furthermore, the database records of access control can be used as data trails when performing audits or monitoring compliance.

4.4.5 Ways to improve access control management at SPU

Participants were asked how access control management could be improved at the university. Participants responded as follows.

According to**SM01,**

> Access control management in the university can be improved through employing more security personnel that will be working in the school compound especially at all access points as this will enable the control of movements and minimise the entrance of unauthorised persons into the university. It will also serve as a means of creating more employment to the masses (SM01).

According to Bitzer and Hoffman (2007), the human element in security systems is often overlooked or neglected completely in the literature. However, this element plays a vital role in security. It is usually humans who make the decision to take action and decide on the type of action to take during a crisis or emergency (Bitzer & Hoffman, 2007). Most technological measures would not be able to function successfully without a human component. For example, if a biometric access control system or smart card is triggered at an organisation, a police official or security guard should respond to observe the use of the system in order for the technological aid to work effectively and to apprehend any intruder. Lombard and Kole (2008) argued that the guard and the security officer are not sufficiently adequate to control access of people to the organisation. It may be inferred that the human security measures expect the guards and security officers to patrol the premises, inspecting and observing the activities taking place and the locations where incidents occur on in order to identify any risks. In this way, the effectiveness of the access control system can be attained.

Another participant, ***Sn01****, stated:*

> It’s been revealed that access control management can be improved through the introduction of biometric system; the introduction of biometric system will enhance the security of the university (Sn01).

Sn03 is in affirmation with **Sn01** adding that

> The introduction of biometric system will make the facilities’ users to be more cautious while accessing the facilities knowing that their activities are taken cognisance of by the university security management (Sn03).

It should be noted that the first biometric used was called soft biometrics established by Bertillon in the nineteenth century (Nixon et al., 2015). Later in the early twentieth century a biometric system using fingerprints was established. From there more studies revolving around biometrics were conducted (Lumini et al., 2016). Innovation played a critical role in advancing the field of biometric access control; more than one feature of a human body can be used to validate access (Nixon et al., 2015).

Furthermore, Teh et al. (2013) highlighted that the biometric access control system includes the network access control which enables someone to gain entrance to a building, identity management control, web management control or remote access control. According to Monwar et al. (2009), the biometric system has the latest technological features to authenticate a person’s identity. Biometric access control has the ability to protect the integrity of personal information, verify an individual’s details and has the potential to eliminate or prevent theft and fraud (Monwar et al., 2009). In addition, Bharadwaj et al. (2015) agree that the biometric system is a mechanism that has the ability to identify the validity of a person using body features like iris, face or fingerprint. Other scholars (Lumini et al., 2016) consider the biometric system to be a technology implemented to identify and verify an individual's unique physical features or interaction characteristics, which provide essential substitutes to a manual access register, smart card or password. The biometric system stores information in the database and nowadays organizations depend on that system to enhance security at entry points of institutions.

The responses of **Sn04** and **Sn06,** "Access control management of the university can be improved through the installation of a boundary fence around the university", support that of **Sn06** who considered that "emphasizing on adding a boom and turnstiles gates as well as a complicated access system will make both the outsiders and the facility users to sit up". The security of the university facilities users is very important hence the management should prioritise it.

From the qualitative data presented, there is an indication that participants want access control management at SPU to be enhanced and improved in order to maintain proper effectiveness in the management at the university. The next section will analyse the quantitative response from the respondents in order to view their opinions on the access control policy management and its effectiveness at SPU.

4.5 QUANTITATIVE DATA ANALYSIS

This section presents the descriptive analysis used in the quantitative research as part of the mixed method research the researcher adopted for the study.

4.5.1 Department and number of staff members

Table 4.5: number of staff

	Frequency	**Percent**	**Valid percent**	**Cumulative percent**
School of Education	40	29.63	29.63	29.63

School of Natural Science	35	25.93	25.93	55.56
School of Economics and Management Science	25	18.52	18.52	74.08
School of Humanities	35	25.93	25.93	100.0
Total	135	100.0	100.0	

From Table 4.5.1it can be deduced that 40 (29.63%) participants from the School of Education participated in the study; 35 (25.93%) participants from the School of Natural Science; 25 (18.52%) from the School of Economics and Management Science; and 35 (25.93%) from the School of Humanities. Hence a total of 135 respondents participated in the quantitative phase of the study.

4.5.2 Rate of returns

This study used a total population of 135 participants, from the School of Education, School of Natural Science, School of Economics and Management Science, and School of Humanities at SPU, Kimberley, Northern Cape Province. Only 90 questionnaires were returned and analysed. Although the researcher tried to ensure more returns, he was unsuccessful. The returned questionnaires were analysed and the results are presented in the tables and figures that follow.

The comprehensive outcome from the SPSS analysis was summarised in Table 4.5.3. The summary presents the general data as obtained from the questionnaires and then the researcher presented the analysed data in a table and bar charts in order to appropriately drive home the research findings with a discussion in relation to the literature of the study.

Table 4.6: Descriptive statistics

	N	Sum	Mean	Std. Deviation	Variance	Skewness		Kurtosis	
	Stat	Stat	Stat	Stat	Stat	Stat	Std. error	Stat	Std. error
Age group	90	162	1.80	.962	.926	1.111	.254	.304	.503
Gender	90	138	1.53	.502	.252	-.136	.254	-2.027	.503
Registered student	90	92	1.02	.148	.022	6.593	.254	42.408	.503
Years spent studying at the university	90	141	1.57	.704	.496	.845	.254	-.529	.503
Faculty enrolled in									
control system at the university									
Control system used to gain access to the university	90	163	1.81	.394	.155	-1.617	.254	.627	.503
Ever been denied access to the university	90	161.00	1.7889	.41038	.168	-1.440	.254	.074	.503
Are the various access control systems at the university effective?	90	107.00	1.1889	.39361	.155	1.617	.254	.627	.503
Reason for ineffectiveness	90	106.00	1.1778	.38447	.148	1.714	.254	.960	.503

Challenges faced at the university on a daily basis with respect to gaining access to the university	90	209.00	2.3222	.81871	.670	-.663	.254	-1.186	.503
Improvements that can help the access control system to avoid access denial to legitimate users	90	227.00	2.5222	1.03019	1.061	.065	.254	-1.132	.503
Valid N (list-wise)	90								

Table 6 presents the numbers and percentages of the participants' responses in relation to the questionnaire distributed for the study. From the above summary and descriptions, it is obvious that 90 questionnaires were completed and unspoiled. The skewness and kurtosis columns work together; hence they depict one another. They show the level of answers selected by the participants regarding the questions in the questionnaire.

4.6 QUANTITATIVE DATA FINDINGS

Quantitative findings helped in understanding the effectiveness of the access control system at Sol Plaatje University, in Kimberley the Northern Cape Province.

Table 4.7: Age group

		Frequency	percent	Valid percent	Cumulative percent
Valid	16 to 21	43	47.8	47.8	47.8
	21 to 25	31	34.4	34.4	82.2
	25 to 30	7	7.8	7.8	90.0
	30+	9	10.0	10.0	100.0
	Total	90	100.0	100.0	

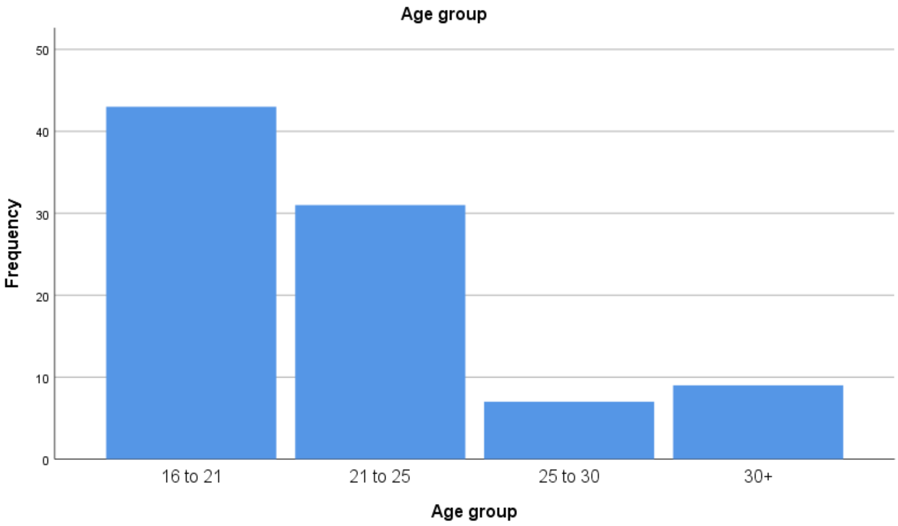
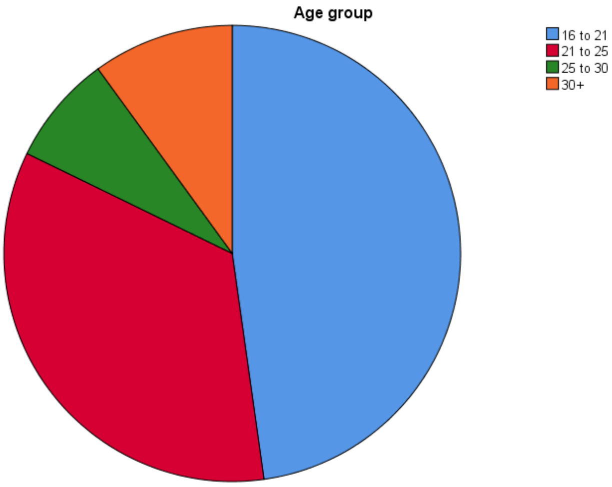


Figure 4..1: Age group



From Table 4.7, Figure 4.1, it can be deduced that 43 (47.8%) participants are aged from 16 to 21 years while 31 (34.4%) of the participants are aged from 21 to 25. A total of 7 (7.8%) participants are between 25 and 30 years of age, while 9 (10%) are 30 years and above.

Table 4.8 Gender

		Frequency	Percent	Valid percent	Cumulative percent
Valid	Male	42	46.7	46.7	46.7

	Female	48	53.3	53.3	100.0
	Total	90	100.0	100.0	

Figure 4.2: Gender

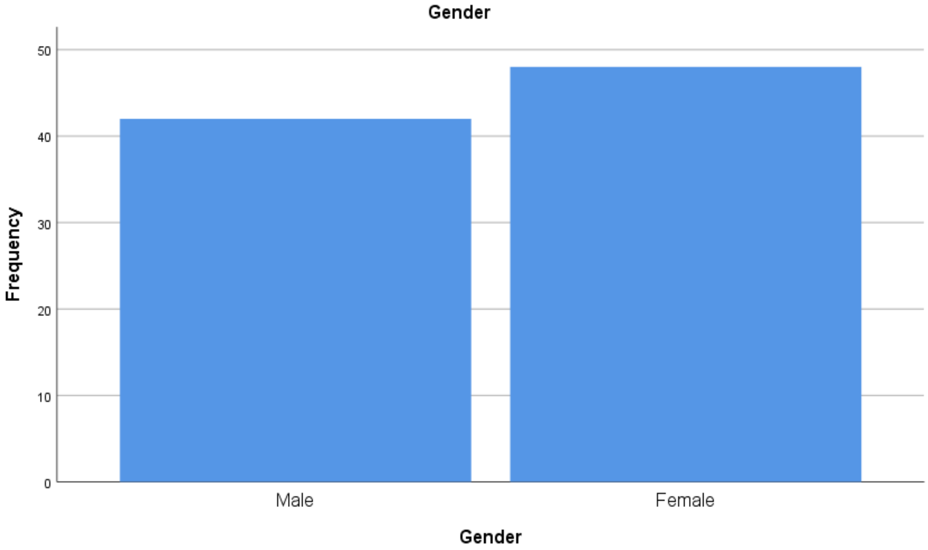


Table 4.8 and Figure 4.2 present the gender ratio of the participants. It is evident that 42 (46.7%) of the participants were male while 48 (53.3%) were female.

Table 4.9 Registered students

		Frequency	Percent	Valid percent	Cumulative percent
Valid	Yes	88	97.8	97.8	97.8
	No	2	2.2	2.2	100.0
	Total	90	100.0	100.0	

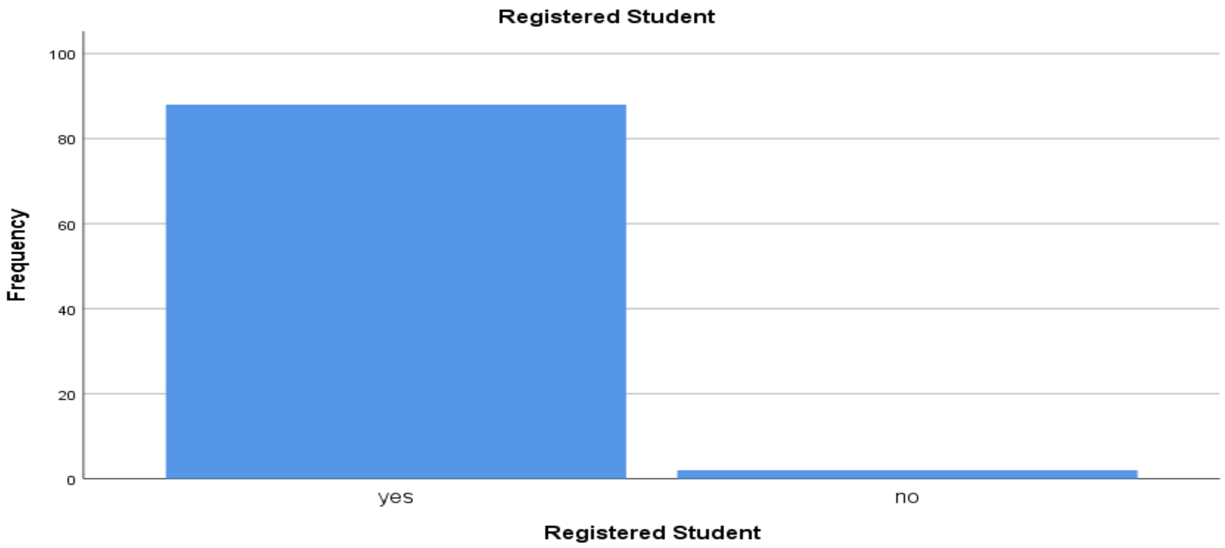


Figure 4.3 registered students

Table 4.9 and Figure 4.3 show that among the participants who took part in the study, 88 (97.8%) were registered students while 2 (2.2%) were not registered at the time of the study.

Table 4.10: Years of study at SPU

		Frequency	Percent	Valid percent	Cumulative percent
Valid	Less than 2 years	50	55.6	55.6	55.6
	2 to 4 years	29	32.2	32.2	87.8
	4 years and above	11	12.2	12.2	100.0
	Total	90	100.0	100.0	

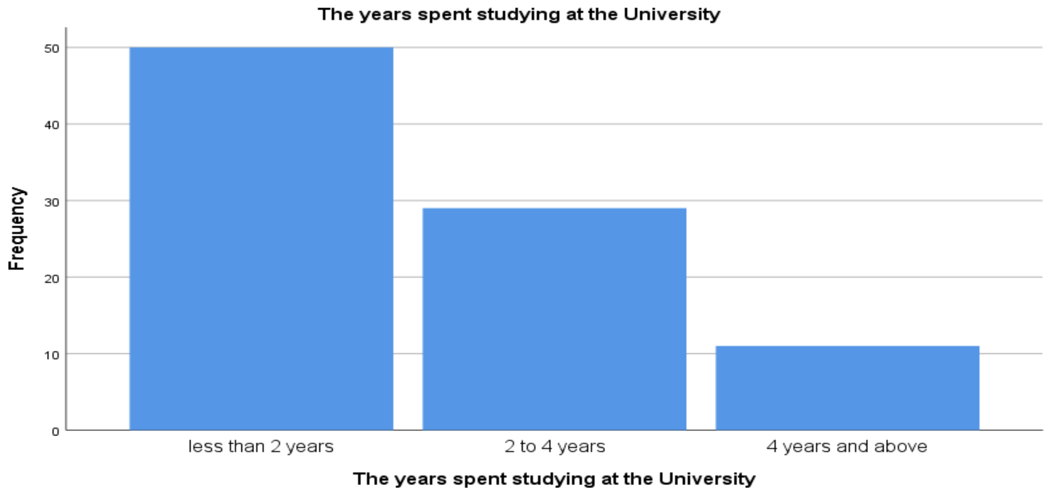


Figure 4.4. Years of study at SPU

This question aimed to determine how long (years) each participant has spent studying at the university. Table 4.10 and Figure 4.4 is a graph showing that 50 (55.6%) of the participants have spent less than 2 years studying at the university; 29 (32.2%) have spent 2 to 4 years at the university while 11 (12.2%) have spent 4 years and above studying at the university.

Table 4.11 Faculty in which enrolled

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Education	45	50.0	50.0	50.0
	Natural Sciences	17	18.9	18.9	68.9
	Economics and Management Sciences	15	16.7	16.7	85.6
	Humanities	13	14.4	14.4	100.0
	Total	90	100.0	100.0	

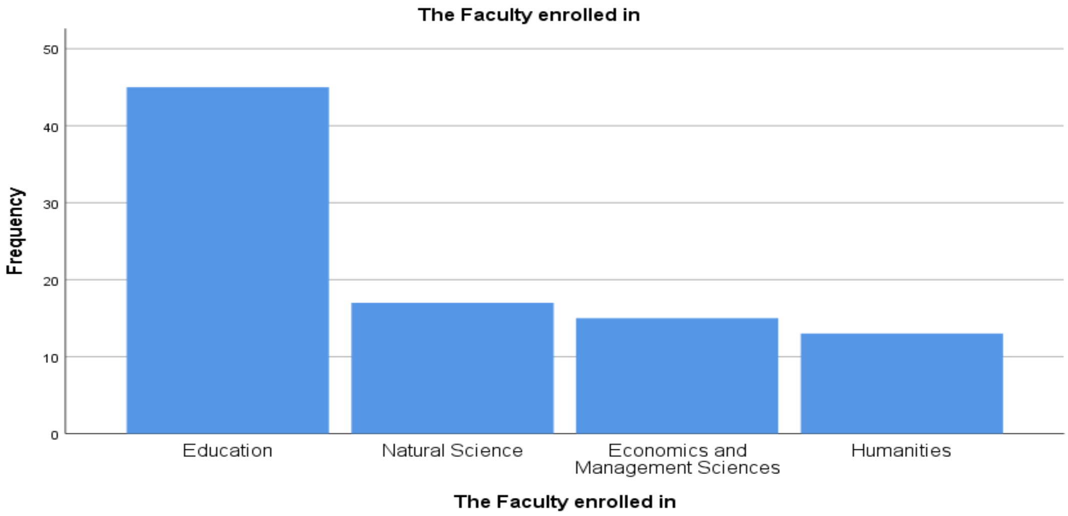


Figure 4.5 Faculty in which enrolled

In order to get generate information regarding the faculty in which participants were enrolled, this question was asked. However, Table 4.11 and Figure 4.5 demonstrate that 45 (50.0%) of the participants are in the Faculty of Education; 17 (18.9%) are in the Faculty of Natural Sciences; 15 (16.7%) are in the Faculty of Economics and Management Sciences, while 13 (14.4%) are in the Faculty of Humanities.

Table 4.12 Access control system

		Frequency	Percent	Valid percent	Cumulative percent
Valid	Yes	87	96.7	96.7	96.7
	No	3	3.3	3.3	100.0
	Total	90	100.0	100.0	

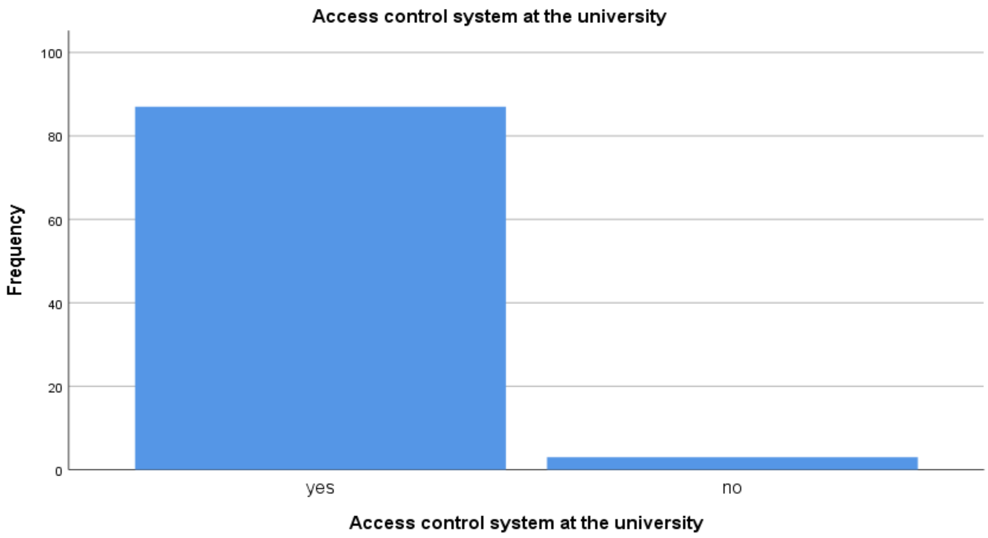


Figure 4.6 Access control system

In order to determine the validity of the access control system used at the university, participants were asked questions. The results are presented in Table 4.12 and Figure 4.6. It is evident that the access control system at the university is valid as 87 (96.7%) of participants gave the answers "Yes" to the question while 3 (3.3%) participants said "No"; the access control system at the university is not valid. The participants' responses mean that the university is doing very well with its access control system as the majority of participants gave an encouraging answer to the question.

Table 4.13: Control system used to gain access to the university

		Frequency	Percent	Valid percent	Cumulative percent
Valid	University website	17	18.9	18.9	18.9
	Using a student card	73	81.1	81.1	100.0
	Total	90	100.0	100.0	

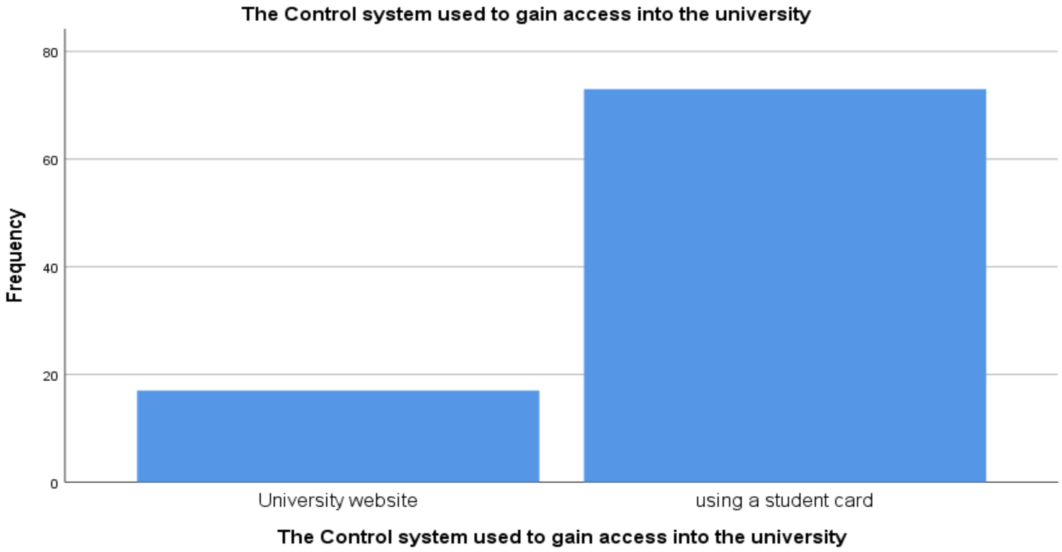


Figure 4.7 Control system used to gain access to the university

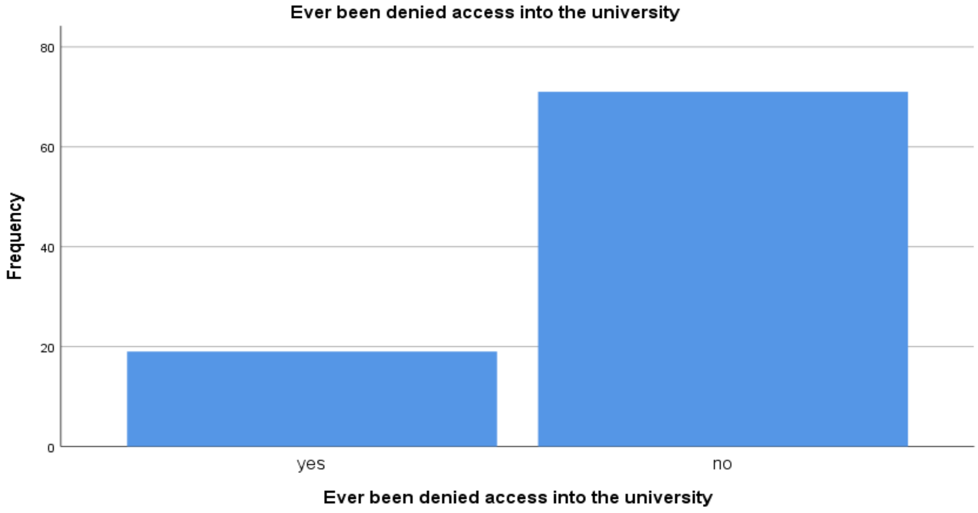
According to Khan (2012), access control systems are becoming more sophisticated because of innovative developments in the field of access control. Hu et al. (2006) defined access control as a technique used for regulating and reporting on individuals who enter and exit an organization's premises with the knowledge of their purpose when entering. Hu et al. (2006) further posit that sufficient safety of information, assets and people is an essential task for the management of an organization. Nixon et al. (2015) agree that a smart card or access card is mostly used in the banking industry, universities and when buying with a credit card. Institutions with an access control system or those intending to put access control in place need to consider developing an access control policy (Hu et al., 2006).

In addition, the access control policy provides firm access control guiding principles that need to be adhered to during implementation. To have a successful access control system, an access control policy is required since it highlights the purpose of the system and specifies the objective with reference to the needs of the organisation. However, in Table 4.13 and Figure 4.7, the question was aimed at ascertaining the type of control system used to gain access to the university by the participants. From Table 4.13 and Figure 4.7, it is clear that 17 (18.9%) respondents mentioned the use of the university website while 73 (81.1%) mention the use of student card as the control system used to gain access to the university. In support of the respondents' response, the Security of Tenure Act 1997 (Act No 62 of 1997) believes that an individual must have legitimate access to an organisation or institution in order to enable proper coordination on the movement within it and in and out of it.. This means that from the data collected, SPU has an access control system such as the use of student cards and websites to gain entrance or exit the institution.

Table 4.14 Ever been denied access into the university

		Frequency	Percent	Valid percent	Cumulative percent
Valid	Yes	19	21.1	21.1	21.1
	No	71	78.9	78.9	100.0
	Total	90	100.0	100.0	

Figure 4.8 Ever been denied access to the university



Gaining access in and out of an organisation is a vital aspect of organisational university security control, however, an unrecognised individual or any of the service users might be denied access to the organisation or university. In this regard, the participants were asked if they had been denied access into the university. Table 4.14 and Figure 4.8 show that 19 (21.1%) of the participants answered, “Yes” that they had been denied access to the university at one point or another while 71 (78.9%) said “No”, they had not been denied access to the university.

Table 4.15: Are the various access control systems at the university effective?

		Frequency	Percent	Valid percent	Cumulative percent
Valid	Yes	73	81.1	81.1	81.1
	No	17	18.9	18.9	100.0
	Total	90	100.0	100.0	

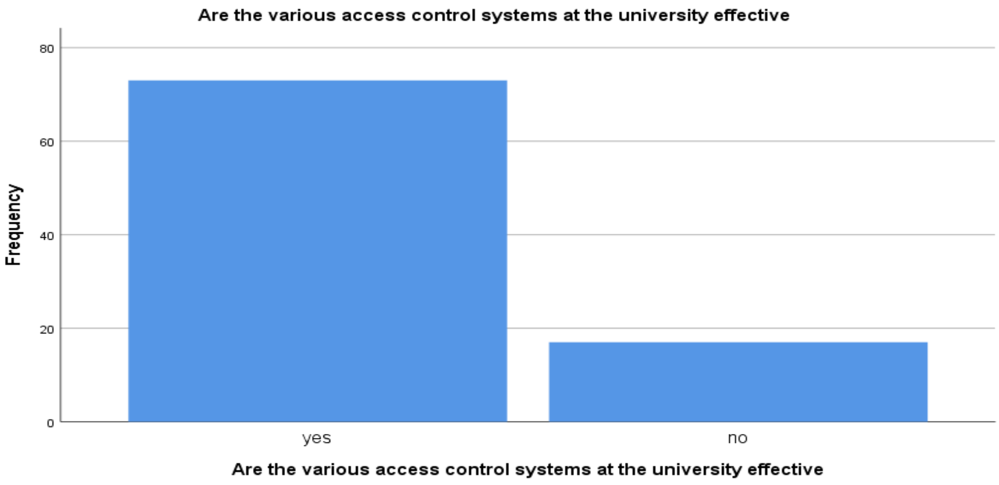


Figure 4.9 Are the various access control systems at the university effective?

According to Sandhu et al. (1996), in order for the access control system to be effective enough, it must provide an appropriate user identity and on the accuracy of the authorisations it needs to regulate access of individuals. It is indispensable to realise that access control is not an absolute solution when it comes to protecting the assets, information, or workers in the jurisdiction of the organisation, although to a certain degree it does play a role in the safety of the organisation. The effectiveness of access control is based on the processes used in an organisation. This process includes the authentication, authorization and audit. Every business implements authentication to one extent or another. Credentials may include a simple user name and password, or more sophisticated authentication like a smart card and PIN. Authorization, on the other hand, allows users access to the appropriate applications, servers, data stores and physical items (such as building doors and equipment) that are within the organisation. Auditing, the third process in access control, creates a user-activity trail. In order to ascertain whether the access control system used at SOL is effective, the participants were asked the relevant questions. Drawing from Table 4.15 and Figure 4.9, it is clear that 73 (81.1%) affirmed that the access control system at the university is effective while 17 (18.9%) replied that it was not effective. However, the finding shows that the university access control system is effective since the majority of the participants agreed to its affectivity. The system control theory on access control in an institution posits that an institution can operate effectively if its access control system is effective and properly managed (Abadi et al., 2014).

Table 4.16: Reason for ineffectiveness

		Frequency	Percent	Valid percent	Cumulative percent
Valid	The system is effective	74	82.2	82.2	82.2
	The system needs improvements	16	17.8	17.8	100.0
	Total	90	100.0	100.0	

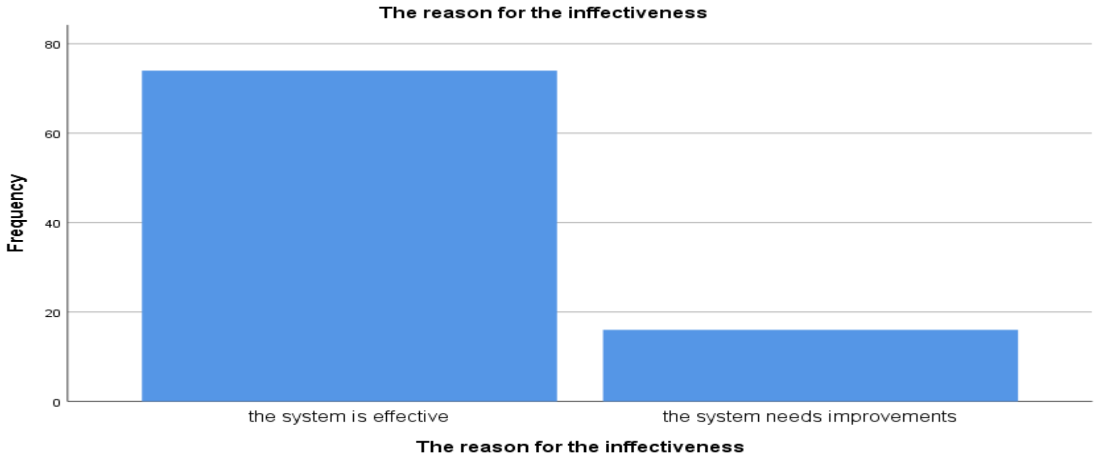


Figure 4.10: Reason for ineffectiveness

In Table 4.16 and Figure 4.10, the findings show the different answers given by the participants regarding the question on the reasons for the ineffectiveness. The question was asked in order to ascertain the reason for the ineffectiveness of the control system. Drawing from the table and figure above, 74 (82.2%) maintained that the control system is effective while 16 (17.8%) suggested that the control system needs improvement. Bigelow (2008) agrees with these findings indicating that the access control system in an organisation needs improvement when there is damage by an unknown user, which means that the access control system is not effective. Furthermore, there is a need for improvement in the access control policy used by such an organisation which would assist to examine if all activities that took place in the access control system complement the initial plan or the set purpose of the system. Audit control is helpful; it has the ability to identify misconduct performed previously; examine the way users act when using the access control system; identify actions that violated the system; and guide or advise in terms of how to prevent misconduct and violation of the system.

In addition, Bigelow (2008) identified that auditing is a measures that can be used to determine whether the access control system is effective or not effective. An audit control is based on empirical analysis of all the requirements and users' actions in the system. In order to perform auditing all the records of the users' actions and are required, together with what should have been performed according to the initial plan. Possible errors in the security of the access control system can be identified during the auditing process. Auditing can also recognise if users abuse their privileges of gaining access to the organisation. Auditing takes place to verify if the system achieves its purpose. If it does not, the access control policy, plan or implementation need to be reviewed in order to complement the objectives of the organisation. In case there is a need to change policy, plan, or the way the system is utilised, efficient change management principles need to be applied.

Moreover, effective security starts with understanding the principles involved in an organisation. Because of its universal applicability to security, access control is one of the most important security concepts to understand. Employees must be aware of the security standards set for an organisation. Hans (2014) argued that most security officers are not aware of the standards of an organisation; hence they need proper training. This is because the property and asset owners or managers desire a safety solution that suits their objectives, in that regard risk to such cannot be tolerated. The management of organisations could benefit tremendously from the continuously growing technology by implementing new IT solutions using change management principles. This implies that management can decide to change an access control policy that does not secure or protect the property of the organisation.

Iconic (2016) indicated that an integrated and structured security risk management plan is essential for all buildings, both business-related and residential, where there are multiple uses or occupancy. An effective and professionally installed access control system must form part of such a management plan. This author also highlighted that modern technology has led to different designs and manufacture of access control systems. However, care must be taken to ensure that these new technologies and applications are suitable and capable for the intended use. Taylor (2017) argued that for effective access control to take place in organisations there is a need to balance effectiveness with operational efficiency, meaning you cannot shut down operations in the name of security. Services need to be provided to constituents but not at the cost of security. Revenues need to be collected, car labels need to be distributed, home improvement inspections need to be done, and police officers need to continue to ensure public safety, and so on. Business has to continue, but at the same time, you need to have adequate security measures in place. The system theory on access control management used in this study also emphasise the need for equating or balancing the effectiveness and the operational efficiency of the organisation in order to ensure security (Cavusoglu et al., 2012). It is essential for the organisation to implement better ways of improving access control management.

Table 4.17 Challenges faced at SPU on a daily basis with respect to gaining access

		Frequency	Percent	Valid percent	Cumulative percent
Valid	Access cards activation	20	22.2	22.2	22.2
	Loss of access cards	21	23.3	23.3	45.6
	No challenges	49	54.4	54.4	100.0
	Total	90	100.0	100.0	

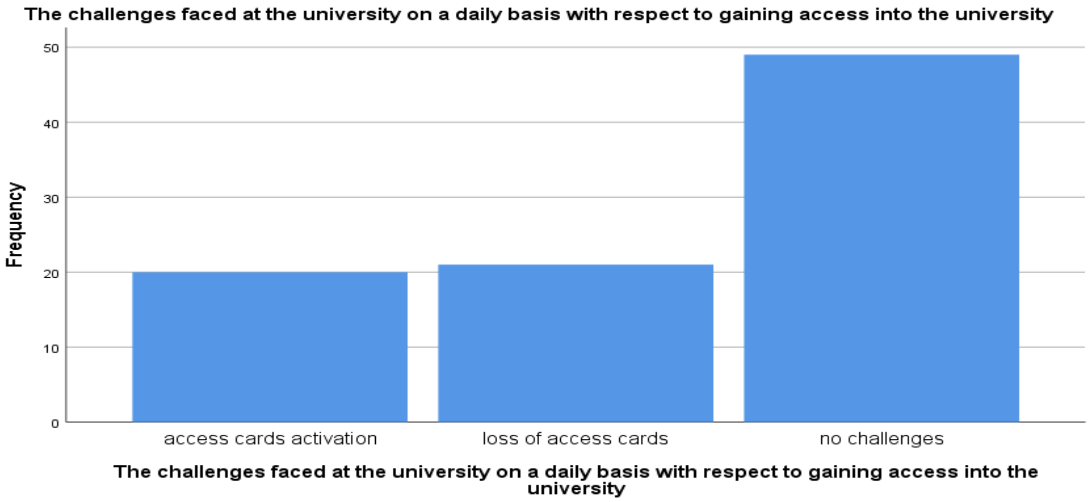


Figure 4.11: Challenges faced at SPU on a daily basis with respect to gaining access

Table 4.17 and Figure 4.11 present the responses from the participants on the challenges faced at the university on a daily basis with respect to gaining access to the university. A total of 20 (22.2%) participants mentioned access cards activation problems; 21 (23.3%) mentioned loss of the access card, while 49 (54.4%) of the participants indicated no challenges. According to Brandewie (2009), there are constant reminders of the threats to our institutions and the vulnerabilities that are raised when a strong programme of identity management has not been implemented in the enterprise. Various challenges on how to implement these access control measures continues to prevail. These challenges include:

- A lack of standardization where organizations are locked into technologies that have failed to keep pace; too many instances of using organization credentials as flash passes for facility access;
- Dynamic response to changing threat levels is another essential challenge; this involves a prepared plan of who needs access during a period of heightened threat and how the authentication and access plan needs to change to raise the security of the access.;
- Managing access privilege: a new generation of smart-badge readers is emerging; these readers are essentially mobile smartcard readers that have been paired with physical access radio frequency identification (RFID) technology. These readers allow the employee, as they approach the access control barriers, to enter a PIN code, which opens the smart card credential. Organisations who have these types of system are struggling on how to manage it. Visitors to the organisation is also a challenge in respect of managing the entry and exit the visitors.

Table 4.18: Improvements that can help the access control system to avoid access denial to legitimate users

		Frequency	Percent	Valid percent	Cumulative percent
Valid	No improvements needed	16	17.8	17.8	17.8
	Introduce fingerprint system	31	34.4	34.4	52.2
	Hire more security officers	23	25.6	25.6	77.8
	Use student numbers for access	20	22.2	22.2	100.0
	Total	90	100.0	100.0	

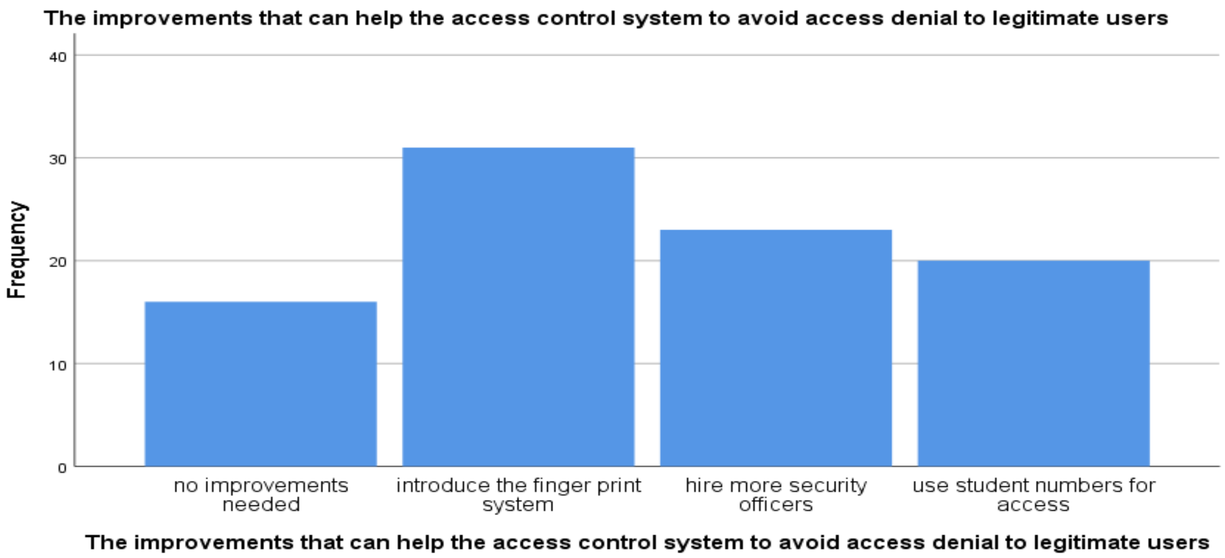


Figure 4.12 Improvements to help the access control system avoid access denial to legitimate users

Table 4.18 and Figure 4.12 present the improvements that could help the access control system to avoid access denial to legitimate users. As indicated by the participants, these improvements when implemented could help SPU to improve the access control system. According to Table 4.18 and Figure 4.12, 16 (17.8%) of the participants indicated that no improvement was needed, hence the control system is working very well. A total of 31 (34.4%) of the participants indicated the introduction of the fingerprint system; 23 (25.6%) also indicated that hiring more security officers would improve the situation, while 20 (22.2%) of the participants indicated the use of student number for access. Hans (2014) proposed the use of fingerprint biometrics stating that the reason behind proposing a fingerprint biometric clocking system is the uniqueness of the features utilised to validate access; no staff member, student or visitor could lose or forget the feature used to gain access. In addition, the feature cannot be stolen. Finally, the fingerprint biometric access control system has been tested to be effective and efficient in other environments (Hans, 2014).

This confirms the findings that use of the fingerprint, as indicated by the respondents, could serve as an effective access control management system at the university. It is important that management ensure that reliable access control systems be used in order to ensure effective management and security at the university.

4.7 CHAPTER SUMMARY

This chapter presented the findings from both qualitative and quantitative data which helped in a broader understanding of the effectiveness of the access control system at SPU in Kimberly, Northern Cape Province. The qualitative findings centred on the access control policy management used at SPU, the challenges faced by SPU in access control management, the perceptions of the students and on access control management used at SPU, the effectiveness of access control policy management used in SPU and the ways to improve access control management at the university. Responses from these questions were made through an interview. This enabled the researcher to obtain an in-depth understanding of the research topic under review.

The quantitative findings, on the other hand, were established from the following: qualitative findings which comprised questions regarding the demographic information of the participants; years spent studying at the university; the faculties in which they studied; access control system at the university; control system used at the university; if the participant has been denied access to the university; effectiveness of the university access control system; reasons for their ineffectiveness; challenges faced at the university on a daily basis with respect to gaining access into the university; and the way to improve the university access control system in order to avoid access denial to legitimate users.

These questions were asked for a broader understanding of the study. The data analysis shows that participants had a good understanding of access control management and there is a good access control system at the university. Although it faces challenges, the university management is addressing them. The data analysis also revealed areas of improvement to enhance the effectiveness of the university access control system. The next chapter deals with the conclusion and recommendations on the effectiveness of the access control system at SPU in Kimberly, Northern Cape Province.

CHAPTER FIVE
CONCLUSION AND RECOMMENDATION

5.1 INTRODUCTION

The main objective of this study is to investigate the effectiveness of the access control system at SPU in Kimberly, Northern Cape Province. Chapter four presented the research findings and discussed them with the relevant literature review that in general, supported the findings. The system theory on access control management was used as the theoretical framework for the study. This theory was also integrated with the discussions of the findings. This chapter presents the overall conclusion of the study findings and recommendations. The chapter was structured in line with the research question and makes conclusions and recommendations. The research questions are:

- What is the access control policy management used in SPU?
- What are the challenges faced by SPU in the access control management?
- What are the perceptions of the students and managements on the access control management used in SPU?
- How effective is the access control policy management used in SPU?
- In what way(s) could access control management be improved in universities?

5.2 ANSWERS TO THE RESEARCH QUESTIONS

5.2.1 What access control policy management is used at SPU?

This question aimed at ascertaining the access control policy management used at SPU. The participants' responses showed that they have good understanding of the university access control policies through their distinctive answers. The researcher backed up the participant's responses with the necessary literature in order to properly drive home the study.

5.2.2 What are the challenges faced by SPU in access control management?

The participants gave their answers based on their understanding of the question as the researcher intended to better understand the effectiveness of the university access control system hence the question on the challenges faced by SPU regarding access control management. The participants' answers show that the university's access control system is effective but that there are challenges. These include strikes, loss of access cards by students, ineffective management of the university turnstiles and unruly behaviour of facility users.

5.2.3 What are the perceptions of students and management on the access control management used at SPU?

Also, the question is aimed at gaining a deeper understanding of the opinion and views of the students and the managers on the access control management used in SPU. The findings revealed that the participants have positive perceptions on the access control management used in SPU. Though one of the participant maintained that the access control system is not necessary since is a university hence everyone should have access to the university.

5.2.4 How effective is the access control policy management used at SPU?

This question aimed at an understanding of the effectiveness of the university's access policy management. The participants responded that the university access management policy has been effective although challenges abound on implementation. However, one participant maintained that the policies are not effective because the university is still new; hence most policies are merely trial and error.

5.2.5 In what way(s) can access control management be improved at universities?

From the qualitative and quantitative data presented and discussed in chapter four, it was revealed that the access control management system in the selected area of study can be improved in a variety of ways. Figure 5.1 shows the key summary of the ways in which access control system could be improved by the management.

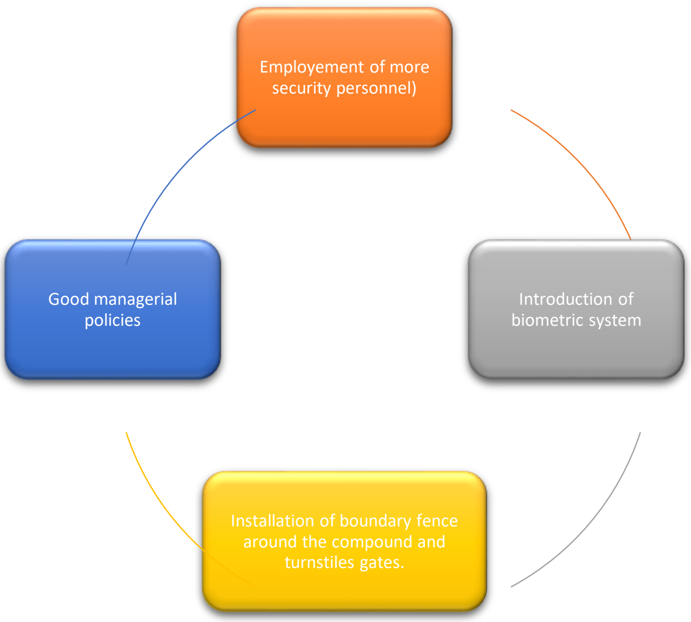

Employement of more security personnel)
Introduction of biometric system
Installation of boundary fence around the compound and turnstiles gates.
Good managerial policies

Figure 5.1: Ways access control policy system can be improved

The findings revealed access control could be improved if the institution employs more security personnel to work on the campus, especially at the access points, introduces a biometric system, and installs a boundary fence around the premises and at the turnstiles gates.

In summary, this research found that the participants had a good understanding of the study and could give an accurate account of their understanding of the project by answering the research questions appropriately. In addition, the study revealed that the access control system used at SPU is effective. Although there are a few challenges opposing its effectiveness, with sound managerial policies these could be overcome. Finally, the study shows that there is a need for further improvement in the university's access control system in order for it to maintain its effectiveness.

5.3 RECOMMENDATION FOR FURTHER STUDIES

Based on the research findings, the following recommendations are made in order to maintain the effectiveness of the access control system:

- Ensure the adequate implementation of access control management policies. When there is efficient implementation of access management policies by the university, there will be a long-lasting effectiveness of the access control system which will make the university more secure.

- Motivate security officers through good salaries and allowances. This would be a motivational measure for security officers in discharging their duties.
- Educate the masses on the need of avoid mass destruction of university properties during a strike.
- Introduce a biometric system to ensure correct record-taking for all who use the facility.
- Introduce a process whereby a senior official of resources grants access to selected staff members to certain areas or locations that are distinct to the institution. This means that there should be an appropriate document to cater for any access to specific areas of the university to which only authorised personnel should have access.
- Provide training to all security staff. This would enable them to understand the policies attached to access control at SPU and the control of the properties of the university.
- Resource managers of the university should control access to important data and regularly review access permissions to allow use of, and access to, important data only where strictly necessary for legitimate business processes.
- Ensure that all students at the university have a card and also follow-up on the correct usage of this card. This could be done by providing rules and policies that will guide the usage of cards students.

5.4 FURTHER RECOMMENDATION

In the interest of the effectiveness of assess control system at universities, it is recommended that further research be done to determine the following:

- Reasons why some students do not follow the policies and procedures on use of the access control system;
- The effect of a lack of adequate access control at a university;
- The reason why some staff members show scant concern on the effective use of the access control system by students of the university.

5.5 CONCLUSION

Chapter one dealt with the introduction of the dissertation, rationale for the study, problem statement, research question and objectives, the significance of the study and the steps required for the study.

Chapter two examined the theoretical foundations of the related research published in this area of interest. It provided an overview of SPU, overview of the access control system in an organisation, importance of access control system in an organisation, policies and statutes applicable in an access control system of an organisation, management methods in controlling the access control system and the challenges managers encounter in controlling access control organisations at large.

Chapter three explored the mixed method research for the study. It gave a description of the research approach, research paradigm, the data collection instrument that was used for the study, the method of analysing the data, and the ethical considerations observed by the researcher.

Chapter four presented the results and findings of the research. With close reference to the literature on the subject, this chapter presented the findings from both qualitative and quantitative data which helped to establish a broader understanding of the effectiveness of the access control system at Sol Plaatje University in Kimberly, Northern Cape Province. The qualitative findings centred on the access control policy management used at SPU, the challenges faced by SPU in access control management, the perceptions of the students and management on the subject, the effectiveness of access control policy management used at SPU and the ways to improve access control management at the university. Responses from these questions were asked through an interview. This enabled the researcher to obtain an in-depth understanding of the research topic under review. The quantitative findings, on the other hand, were derived from the qualitative findings. They were comprised of questions regarding the statistics of the participants' demographic information, and other research questions that aided the study.

Findings from the qualitative data collected helped the researcher to shed more light on the qualitative findings.

Chapter five combined all insights from the previous chapters into a conclusion of the results with recommendations for future research. This dissertation presented an account of the effectiveness of access control policy system in the organisation. Finally, the researcher proposed a number of recommendations.

REFERENCES

Ackroyd, S. & Hughes, J.A. 2010. *Data collection in context*. Thousand Oaks: Longman.

Anil, K.J., Nandakumar, K. & Nagar A. 2008. *Biometric Template Security*, 2008; Article ID 579416, 1-17.

Barbour, R. 2008. *Introducing qualitative research: A student guide to the craft of doing qualitative research*. London: Sage.

Bauer, L., Cranor, L.F., Reeder, R.W., Reiter, M.K. & Vaniea, K., 2009, April. Real life challenges in access-control management. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 899-908). ACM.

Bednarek, M., Dabrowski, T. & Wisnios, M. 2013. Credibility analysis of a multi-biometric identification system for fingerprints. Military University of Technology, Warsaw, 105-115.

Bharadwaj S., Bhatt H.S., Singh, R., Vatsa, M., Noore, A. 2015, QFuse: Online learning framework for adaptive biometric system, 48, 3428–3439.

Bitzer, E.G. & Hoffman, A. 2007. Psychology in the study of physical security. *The Journal of Physical Security, 1*(2): 1-18. Available at: http://jps.lanl.gov/vol.2/4-Psychology_and _security.pdf. Accessed on 27/09/2017.

Brandewie, R. 2009. New challenges for access control. Available at: https://www.scmagazine.com/new-challenges-for-access-control/article/556281/. Accessed 25/08/2017.

Brynard, P.A. & Hanekom, S.X. 2005. *Introduction to research in public administration and related academic disciplines.* 3rd edn. South Africa, Pretoria: Van Schaik.

Carrtegra, L.L.C. 2015. Effectiveness of access control. Available at: http://www.carrtegra.com/2015/06/8-ways-to-ensure-effective-system-access-controls/. Accessed 24/08/2017.

Chung, C.K. 2001. A biometric identification system by extracting hand vein patterns. *Journal-Korean Physical Society* (38)3, March 2001, 268-272.

Cooper, D.R. & Schindler, P.S. 2011. *Business research methods.* 3rd edn. United Kingdom, Berkshire: McGraw-Hill Education.

Creswell, J.W. 2013. *Qualitative inquiry and research design: Choosing among the five approaches*. Thousand Oaks, CA: Sage.

Creswell, J.W. 2014. *Research design: Qualitative, quantitative and mixed methods approaches*. 4th edn. Thousand Oaks, CA: Sage.

Creswell, J.W., Maree, K., Ebersohn, L., Ellof, I., Ferreira, R., Ivankova, N.V., Jansen, J.D., Niewenhuis, J., Pietersen, J., Plano Clark, V.L. & Van der Westhuizen, C. 2007. *First steps in research.* Pretoria: Van Schaik.

Edmonds, J. 2011. Managing successful change. *Industrial and Commercial Training*, 43(6), 349-353.

Ferraiolo, D.F., Sandhu, R., Gavrila, S., Kuhn, D.R. and Chandramouli, R., 2001. Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security (TISSEC)*, *4*(3), pp.224-274.

Gafurov, D., Helkala, K. & Sondrol T., 2006, Norwegian Information Security Lab – NISlab, Biometric Gait Authentication Using Accelerometer Sensor, 1 (7), 1-9.
http://www.biometricupdate.com/201501/history-of-biometrics (07/07/2016).
http://www.spu.ac.za/ (05/08/2016).

Graves, D. & Mirsky, L. 2007. American Psychological Association report challenges school zero-tolerance policies and recommends restorative justice. International Institute for Restorative Justice. Available at: http://fp.enter.net/restorativepractices/apareport.pdf. Accessed 07/09/2017.

Hu, V.C., Kuhn, D.R., Ferraiolo, D.F. and Voas, J., 2015. Attribute-based access control. Computer, 48(2), pp.85-88.

Kallet, R.H., 2004. How to write the methods section of a research paper. Respiratory care, 49(10), pp.1229-1232.

Khan, M.K. & Zhang, J. 2007. Improving the security of 'a flexible biometrics remote user authentication scheme'. *Journal of Physical Security*. 29, 82–85.

Khan, S.R. 2012. Development of low-cost private office access control system *OACS*; *2*(2), 1-7.

Kuhn, D.R., Coyne, E.J. & Weil, T.R. 2010. Adding attributes to role-based access control; *Sensors*, *10*(3), pp. 79-81.

Lekganyane, S.A. 2011. Managing learners' misconduct in Ntoane Village Secondary School. MEd dissertation: University of South Africa.

Lumini, A. & Nanni, L. 2016. Overview of the combination of biometric matches. *Sensor;* 33, 71–85.

Maree, K. 2010. *First steps in research*. Pretoria: Van Schaik.

Marshall, C. & Rossman, G.B. 2011. *Designing qualitative research.* 5th edn. California: Sage.

May, L. and Lane, T., 2006. A Model for improving e-Security in Australian Universities. *Journal of Theoretical and Applied Electronic Commerce Research*, *1*(2).

McAndrews, T. 2001. Zero-tolerance policies. Available at: http://eric.uoregon.edu/publications/digests/digest146.html. Accessed 02/10/2017.

McMillan, J.H. & Schumacher, S. 2010. *Research in education: Evidence-based inquiry*. 7thedn. Boston, MA: Pearson.

Monwar, M.M. and Gavrilova, M.L., 2009. Multimodal biometric system using rank-level fusion approach. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, *39*(4), pp.867-878.. 7-9.

Muhammad, I.S., Peter, B., Jia Xu & Elisa B. 2016. *A comprehensive access control system for scientific applications, electrical and computer engineering.* Purdue University. Cyber Center, Purdue University. Computer Science, Purdue.

Nigam, I., Vatsa, M. & Singh, R. 2015. Ocular biometrics: A survey of modalities and fusion approaches*. Information Fusion,* 26, 1–35.

Nixon, M.S., Correia, P.L., Nasrollahi, K., Moeslund, T.B., Hadid, A. Tistarelli M., 2015. On soft biometrics; *Journal of Theoretical and Applied Electronic Commerce Research* 68, 218–230.

Patil, A. and Meshram, B.B., 2012. Database Access Control Policies. *Database*, *2*(3), pp.3150-3154.

Patrick, V. & Fiel, S. 2013. Access control is a vital part of campus security. Available at https://www.universitybusiness.com/article/access-control. Accessed 9/08/2017

Popper, K. *The logic of scientific discovery* (1959), reprinted (2004). Routledge, Taylor & Francis.

Republic of South Africa. *Trespass Act of 1959 (No. 6 of 1959)*, South Africa, Pretoria: Government Printer.

Republic of South Africa. 2005. Draft National Policy Framework for Public Participation. Pretoria: Government Printer.

Republic of South Africa. Department of Education. 2009. Education statistics in South Africa 2007. Available at: http://www.education.gov.za/emis/emisweb/statistics.htm. Accessed 01/03/2010.

Riera, A., Soria-Frisch, A., Caparrini, M., Grau, C. and Ruffini, G., 2008. Unobtrusive biometric system based on electroencephalogram analysis. *EURASIP Journal on Advances in Signal Processing*, *2008*, p.18.

Rogers, C. & Schoeman, J. 2010. Security practice III: SEP3701, Units 1-5. Pretoria: University of South Africa.

Rossman, G.B. & Rallis, S.F. 2012. *Learning in the field: An introduction to qualitative research*. 3rd edn. Sage publication.

SABC. 2017. Fees must fall protest. Available at http://www.sabc.co.za/wps/portal/news/main/tag?tag=Fees%20Must%20Fall. Accessed 24/08/2017.

Sandhu, R. and Samarati, P., 1996. Authentication, access control, and audit. *ACM Computing Surveys (CSUR)*, *28*(1), pp.241-243.

Solus, M. 2016: Advanced access control and security. Available at: http://www.solus.co.in/isolus/?gclid=Cj0KCQjw5arMBRDzARIsAAqmJeyQzKKkx9JEMrrVbblc3Ce_Z0zIDQVPMVtek3RMIEPM75XJMZPJkMYaAh2LEALw_wcB. Accessed 6/08/2017.

Stephen J. 2008. The importance of access control. Available at: :http://searchitchannel.techtarget.com/feature/The-importance-of-access-control. Accessed 24/08/2017

Sungau, J.J., Ndunguru, P.C., Kimeme J. 2013. Business process re-engineering: The technique to improve speed of service industry in Tanzania, 4(1) 236-269.

Teh, P.L., Ling, H.C. & Cheong, S.N. 2013. NFC Smartphone-based access control system using information-hiding, 2013, 2–4.

Tong, Q., Zhang, H. & Sun, G. 2011, Design and execution scheme of the access control system of university based on CPU card. *Computer Engineering and Design; 32*(4), 1453-1457.

Tuyls, P. & Batina, L, 2006. RFID-Tags for anti-counterfeiting, 3860/115-131.

Welman, J.C., Kruger, S.J. & Mitchell, B.C. 2005. *Research methodology*. 3rd edn. South Africa, Cape Town: Oxford University Press, Southern Africa (Pty) Ltd.

Williams, C. 2007. Research methods, *5*(3), 65-72.

Wilson, E. & Fox, A. 2009. Collecting data for school-based research: A guide for education students, *Journal on Advances in Signal Processing*, 76.

Yeh, S., Luo, Y., Zhao J. & Cheung S. 2009. Anonymous biometric access control, (2), 10.1155/2009/865259.

APPENDIX A: INTERVIEW GUIDE

INVESTIGATING THE EFFECETIVENESS OF THE ACCESS CONTROL SYSTEM AT SOL PLAATJE UNIVERSITY, IN KIMBERLEY THE NORTHERN CAPE PROVINCE

INTERVIEW GUIDE FOR SECURITY OFFICERS AND MANAGERS

1. How long have you been working as a security manager/officer for the university?
2. What do you understand by access control at the university?
3. Are there any access control policy used in the university? If yes, what are these policy?
4. What are the challenges faced by the university in managing access control in the school?
5. Do you think the access control policy used by the university is strict enough? Please explain your answer.
6. What are your perceptions on the access control policy used in the university?
7. Is the access control policy used effective? If yes, explain how effective it is in the university?
8. In what way(s) can the access control management be improved in the university?

APPENDIX B

QUESTIONNAIRE FOR STUDENT

EFFECTIVENESS OF ACCESS CONTROL

1. How long have you been studying in the university?

   Less than 2 years □

   2- 4 year □

   4 years and longer □

2. Gender : Male □

   Female □

3. Please indicate your age in bracket

   16-21 □

   21-25 □

   25-30 □

   30+ □

4. Which Faculty are you?

   Education □

   Natural science □

   Economics and management science □

   Humanities □

5. Have you been denied access to the school? If yes, indicate your reason in the box below

   Yes □

   No □

6. There are various Biometric access control system that can be employed at the universities. Please indicate which one is used in SPU.

   Network access control □

Identity card management □

Web access control □

Remote access control □

Other please specify

7. Do you think the access control management is effective in the university? If no, please indicate the reason for its ineffectiveness.

   Yes □

   No □

8. What are the challenges faced by the university in respect of access control management?

9. The following are ways in which access control management can be improved. Please indicate which you would suggest for the school.

   Network access control □

   Identity card management □

   Web access control □

   Remote access control □

   Others please specify

10. Please indicate the reason(s) behind the access control system you suggested for the university

THANK YOU FOR PARTICIPATING