



**UNIVERSITY OF KWAZULU-NATAL**

**THE IMPACT OF GOVERNMENT EMPLOYEES USING BIOMETRICS IN IT  
SECURITY MANAGEMENT AT KZN TREASURY**

**Student name**

**Nomkhosi Ndaba**

**Student number**

**217079556**

**A Thesis for the degree of Masters of Commerce (Course Work)**

**College of Law and Management Studies**

**School of Management, Information Technology and Governance**

**Supervisor name**

**Dr Trishana Ramluckan**

**Year:**

**2019**

## DECLARATION

I Nomkhosi Ndaba declare that:

- (i) The research reported in this dissertation/thesis, except where otherwise indicated, is my original research.
- (ii) This dissertation/thesis has not been submitted for any degree or examination at any other university.
- (iii) This dissertation/thesis does not contain other persons' data, pictures, graphs or other information, unless specifically acknowledged as being sourced from other persons.
- (iv) This dissertation/thesis does not contain other persons' writing, unless specifically acknowledged as being sourced from other researchers. Where other written sources have been quoted, then:
  - a) their words have been re-written but the general information attributed to them has been referenced;
  - b) where their exact words have been used, their writing has been placed inside quotation marks, and referenced.
- (v) Where I have reproduced a publication of which I am author, co-author or editor, I have indicated in detail which part of the publication was actually written by myself alone and have fully referenced such publications.
- (vi) This dissertation/thesis does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the source being detailed in the dissertation/thesis and in the References sections.

Signed: \_\_\_\_\_

## **ACKNOWLEDGEMENTS**

Most praise to the almighty God, this would not be possible without his grace and the strength he has provided me. I would like to express my sincere gratitude and appreciation to the following individuals who have contributed to my success regarding my studies:

- My beloved husband Bonga Ndaba and our lovely daughter Yamkela Ndaba for their support and encouragement;
- My mother Ms Nomusa Mthembu and sister Ms Nonhlanhla Mthembu for their encouragement;
- My in-laws' Dr and Mrs Ndaba and sister in-law Ms Thabile Ndaba for their inspiration;
- Mr Simiso Magagula, the Head of the Department of KZN Treasury, who had granted me approval to conduct the study at the KZN Treasury department;
- My supervisor, Dr T Ramluckan for the ongoing support that she has shown me throughout this study;

## CONTENTS

Abstract .....	10
Key Terms .....	12
CHAPTER 1 .....	13
1.1 Introduction.....	13
1.2 Background .....	13
1.3 Evidence of Problem Exist.....	14
1.4 Urgency of Study .....	14
1.5 Body of Knowledge Contribution.....	14
1.6 Research Problem .....	14
1.7 Security Management in KZN Treasury.....	15
1.8 Magnitude of the Problem .....	15
1.9 Research Questions .....	16
1.10 Research Objectives.....	16
1.11 Significance/importance/contribution of the study .....	16
1.12 Justification of the study .....	17
1.13 Research Methodology .....	17
1.14 Research Design.....	17
1.15 Research Approach .....	18
1.16 Ethical Considerations .....	18
1.17 Conclusion .....	18
CHAPTER 2 .....	19
2.0 LITERATURE REVIEW AND THEORETICAL FRAMEWORK .....	19
2.1 Introduction.....	19
2.2 Security Management in KZN Treasury.....	19
2.3 Biometrics System .....	20
2.4 Different Types of Sectors using Biometrics.....	23
2.4.1 Biometrics in Banking .....	23
2.4.2 Biometrics in E-voting.....	25
2.4.3 Biometrics Attendance Recording system (BARS).....	25
2.4.4 Biometrics in Travel .....	26
2.5 Features of Biometrics .....	27
2.6 Employees' perceptions in using Biometrics.....	29
2.7 Training needs.....	30
2.8 Technology Adoption .....	30
2.9 Advantages and Disadvantages.....	31

2.9.1 Advantages.....	31
2.9.2 Disadvantages .....	31
2.10 Theoretical Framework.....	32
2.10.1 The Technology Acceptance Model .....	32
2.10.2 DeLone and McLean (1992) Model .....	33
2.11 Conclusion .....	33
CHAPTER 3 .....	35
3.0 RESEARCH METHODOLOGY.....	35
3.1 Introduction.....	35
3.2 Research Method .....	35
3.3 Reasons for selecting this Research Method .....	36
3.4 Research Design.....	36
3.5 Research Methods .....	37
3.6 Data Collection and Analysis.....	38
3.7 Sampling Strategy .....	39
3.7.1 Probability Sampling .....	39
3.7.2 Non-Probability Sampling.....	39
3.7.3 Sampling Technique .....	40
3.8 Instrument Design.....	41
3.8.1 Questionnaires.....	41
3.9 Data Collection .....	42
3.10 Methods of Data Analysis.....	42
3.11 Ethical Considerations .....	43
3.12 Problems and Limitations .....	44
3.13 Conclusion .....	44
CHAPTER 4 .....	45
4.0 DATA ANALYSIS AND INTERPRETATION .....	45
4.1 Introduction.....	45
4.2 Sample Characteristics.....	45
4.3 SECTION A: Demographic profile of respondents.....	45
4.3.1 Gender of the respondents .....	45
4.3.2 Current Employment Position.....	46
4.3.3. Qualification .....	47
4.3.4 Gender by the highest qualification .....	48
4.3.5 Gender by the position in the organization .....	50
4.4 SECTION B: Perceived Usefulness of Biometrics in System and Information Quality ...	51

4.5 SECTION C: Perceived Ease of Use of Biometrics, User Satisfaction and Individual and Organization Impact.....	57
4.6 SECTION D: Influencing Factors for use of Biometrics.....	63
4.7 SECTION E: Technology Used.....	69
4.4 Conclusion .....	75
CHAPTER 5 .....	77
5.0 CONCLUSION AND RECOMMENDATIONS .....	77
5.1 Introduction.....	77
5.2 Objectives of the Study.....	77
5.3 Population of the Study.....	77
5.4 Cronbach's Alpha .....	78
5.5 Findings of the Study .....	79
5.6 Recommendations.....	83
5.7 Limitations and Implications for further research .....	84
5.8 Conclusion .....	85
5.9 References.....	87
APPENDIX.....	90
Appendix 1: Gatekeeper Letter .....	90
Appendix 2: Ethical Clearance Letter.....	92
Appendix 3: Informed Consent Form .....	93
Appendix 4: Questionnaire .....	96

## LIST OF FIGURES

Figure 2.1: The Technology Acceptance Model.....	33
Figure 2.2: The DeLone and McLean (1992) Model.....	33
Figure 4.1 Gender .....	46
Figure 4.2: Employment Position .....	47
Figure 4.3: Qualification.....	48
Figure 4.4: Gender highest Qualification.....	49
Figure 4.5: Gender and Position .....	50
Figure 4.6: Biometrics improves the quality of work .....	52
Figure 4.7: Biometrics provides greater control over the work .....	53
Figure 4.8: Biometrics enables system security control .....	54
Figure 4.9: Biometrics provides a greater organizational impact .....	55
Figure 4.10: Biometrics provides accurate information .....	56
Figure 4.11: Ease of use of biometrics finger print as security measure .....	58
Figure 4.12: Biometrics as an unnecessarily complex.....	59
Figure 4.13: Easy use of biometrics.....	60
Figure 4.14: Biometrics as a monitoring and tracking tool rather than a security tool.....	61
Figure 4.15:Biometrics provides accountability .....	62
Figure 4.16: Biometrics security adds value to service delivery .....	64
Figure 4.17: Biometrics builds a good impression on employees .....	65
Figure 4.18: Re-enrolment and enrolment of multiple fingers mitigates errors .....	66
Figure 4.19: Individuals being responsible in their actions and activities .....	67
Figure 4.20: Characteristics and challenges that makes difficult for decisions making .....	68
Figure 4.21: Latest technology used for security control .....	71
Figure 4.22: KZN Treasury using the most secured and latest technology in managing security .....	72
Figure 4.23: Biometrics fingerprint feature provides an accurate security control .....	73
Figure 4.24: Technology used to provide a secured and reliable user identity.....	74
Figure 4.25:Using the latest technology makes users feel at ease .....	75

## LIST OF TABLES

Table 3.1: Number of participants .....	38
Table 3.2: Total number of participants.....	40
Table 3.3: Group classification .....	41
Table 4.1: Gender frequency.....	46
Table 4.2: Employment position frequency.....	47
Table 4.3: Qualification frequency .....	48
Table 4.4: Gender highest qualification.....	49
Table 4.5: Gender and Position.....	50
Table 4.6: Summary of question responses in section B .....	51
Table 4.7: Biometrics improves quality of work .....	52
Table 4.8: Biometrics provides greater control over the work .....	53
Table 4.9: Biometrics enables system security control.....	54
Table 4.10: Biometrics provides a greater organizational impact .....	55
Table 4.11: Biometrics provides accurate information.....	56
Table 4.12 Summary of question responses in section C .....	57
Table 4.13: Ease of use of biometrics fingerprint as security measure .....	58
Table 4.14: Biometrics as an unnecessarily complex .....	59
Table 4.15: Easy use of Biometrics .....	60
Table 4.16: Biometrics as a monitoring and tracking tool rather than security tool.....	61
Table 4.17: Biometrics provides accountability .....	62
Table 4.18: Summary of question responses in section D .....	63
Table 4.19: Biometrics security adds value to service delivery.....	64
Table 4.20: Biometrics builds a good impression on employees.....	65
Table 4.21: Re-enrolment and enrolment of multiple fingers mitigates errors.....	66
Table 4.22: Individuals being reliable in actions and activities.....	67
Table 4.23: Characteristics and challenges that makes difficult for decision making.....	68
Table 4.24: Summary of question responses in section E .....	70
Table 4.25: Latest technology used for security control.....	70
Table 4.26:KZN Treasury using the most secured and latest technology .....	71
Table 4.27: Biometrics fingerprint feature provides accurate security control .....	72
Table 4.28: Technology used provides a secured and reliable user identity .....	73



Table 4.29: Using the latest technology makes users feel at ease .....	74
Table 5.1: Case processing summary.....	78
Table 5.2: Cronbach's alpha the reliability statistics.....	78
Table 5.3: Reliability statistics.....	78
Table 5.4: Summary item statistics .....	79

## **Abstract**

The aim of this study is to analyse the different opinions, draw up a balance, and determine the impact of biometrics on users that are using it as their IT security control, especially in financial systems that are used at KZN Provincial Treasury viz Basic Accounting System and Persal. It outlines the strengths and weaknesses, as well as discover the theoretical or conceptual frameworks to be used to examine this phenomenon. This study will assist in enabling to determine impact of using the Biometrics security technology on employees of the KZN Treasury.

Today biometrics has been successfully deployed in various fields like security, identification and authorization system. Biometrics fingerprint has gained significant importance in this technical world for analysing of biological data. Biometrics is a technology that is used for analysing person characters based on physiological traits such as the face, fingerprint, iris, retina, voice, signature, etc. The KZN Treasury introduced biometrics systems to increase security on Basic Accounting System and Persal. Biometrics serves as a crucial point to resolve issues relating to personal identification and verification technology. The Biometrics fingerprint is used to establish one's identity in order to minimize fraud within Government Departments. It ensures that acceptable access measures are implemented to protect crucial systems by providing secured access control. The biometrics system at KZN Treasury prevents information loss and unauthorised access and ensures that adequate non-repudiation measures are implemented. It also gives an audit trail of sensitive transactions with the information kept in a secured and protected database.

The quantitative method is used for collecting data. The research tool used was a questionnaire with three groups of participants the managers, enrolment officers and employees or users. The five-point Likert scale questionnaire is used to gather the relevant data for analysis and interpretation as well as drawing relevant conclusions and recommendations. The findings in this study were analysed in detail to be able to produce a precise data analysis. The conclusion of the study is that the use of the Biometrics security system has created a good impact on the work performance of the employees of the KZN Treasury. It seems that most of the respondents believe that Biometrics has had a significant and positive effect on the level of work performance. This study only touches on four areas of Biometrics, which are Perceived

Usefulness, Perceived Ease of Use (user satisfaction and organizational impact), Influencing Factors and Technology and Security. This study is not aimed to cover a full and detailed list of biometric techniques.

***Keywords:*** Biometrics, IT Security Management, Basic Accounting System, Persal system, Information Communication Technology

**Key Terms**

ATM: Automated Teller Machine

Authentication: Means being accepted in the application

BAS: Basic Accounting System

Biometrics: System that involves pattern recognition

BARS: Biometric Attendance Recording System

ICT: Information Communication Technology

IEBC: Independent Electoral and Boundaries Commission

IPCR: Individual Performance Commitment Review

IS: Information Systems

KZN: KwaZulu-Natal

LGU: Local Government Unit

Persal: Payroll System and Leave Management

PKI: Public Key Infrastructure

Security: Means protection of information

# CHAPTER 1

## 1.1 Introduction

This study is determining the impact of Government Employees using Biometrics in IT Security Management at the KZN Treasury. The reason for this study is also to determine whether IT security is being compromised in the departments in order to minimize fraud. This will be done by interviewing employees that are using biometrics for IT security and establishing if they find the system easy to use. The biometrics system is used to establish one's identity in order to minimize fraud. The study determines whether the failure to comply with IT Security Management will compromise data and exposed it to unauthorized users of the system. Using Biometrics will assist in providing quality and better service delivery in the departments and minimize fraud. Employees in the KZN Treasury have different opinions regarding biometrics security devices. Some regards biometrics security devices as an invasion of their privacy and confidentiality, but Management is grateful for the additional security and the essential responsibility and reliability that this system has provided.

Some employees would prefer not to use biometrics since they have labelled it as an invasion of their privacy and confidentiality and they don't agree with the implementation of biometrics, saying it should not be used. Biometrics system consist of these methods: face recognition, fingerprint identification, hand geometry, retina scan, iris scan, signature and voice analysis but my study is based on fingerprint identification, since it is the only one that is used at KZN Treasury. With the use of biometrics at KZN Treasury, fraud levels are decreasing.

***Research Topic: The impact of Government Employees using Biometrics in IT Security Management at KZN Treasury.***

## 1.2 Background

KZN Treasury provides an important function in implementing and supporting the information systems within the province. Biometrics is critical to guarantee that the ICT networks and support systems are sufficiently secure. Currently, KZN departments are experiencing a huge problem with fraud, therefore, Biometric access control has been introduced at KZN Government Departments to enhance access controls in order to reduce fraud Biometric control also improves the acceptability and accountability pertaining to the Basic Accounting System and Persal systems. Biometrics has been used as the gateway to BAS and Persal Systems within KZN

departments. Without biometrics, users cannot access BAS or Persal to perform their duties. Biometrics is utilized to identify users on their actions, tendencies (Purgason and Hibler, 2012).

### **1.3 Evidence of Problem Exist**

This study is based on reliability, security and impact issues related to biometric authentication. The access methods and security are changing constantly with technology. In this day and age, a key is not the only way to unlock doors (there are key cards, pin codes, and other methods). There is a continuous need to improve security and controls. This has formed a strong necessity for consistent identity management.

The problem that exist is that there is a need to identity and verify an individual's actions in order to prevent fraud. The common control-based identification approaches used are identity cards, tokens, keys or knowledge created methods such as a password or a PIN. The problem is that passwords can easily be stolen, shared or forgotten, which results in compromising identity in the form of identity theft.

### **1.4 Urgency of Study**

There is a need to conduct this study to be able to assess and measure the perspectives and the impact of using the Biometrics security technology on employees of the KZN Treasury. The urgency is also to verify and evaluate whether fraud and theft are increasing or decreasing. There was a need for this study to be conducted to ensure effective service delivery and measure controls.

### **1.5 Body of Knowledge Contribution**

This study contributes to the body of knowledge since it provides a clear vision concerning the use of biometrics and resolve issues regarding employees' attitude towards biometrics security system.

### **1.6 Research Problem**

This study is to assess the impact of Biometrics on government employees at KZN Treasury. The research problem is to identify the impression that the Biometric access control system has created at KZN Treasury. Furthermore, to identify improvements regarding the acceptability and accountability pertaining to the use of BAS and Persal systems on the employees through the use of biometrics. The systems accessibility is crucial as all the users, need biometrics to enable them

to accomplish their functional duties. Some employees, however, feel that it is a way to invade their privacy and to monitor them.

### **1.7 Security Management in KZN Treasury**

Biometrics technology has improved the security control in systems at KZN Treasury for years; it enables the tracking of individual physical characteristics for identity identification in order to prevent identity theft.

The biometrics security systems for KZN Treasury has an innovative feature that permits individuals to access the system once the biometric scanning unit has identified that individual through the method of specific inherent characteristic. One such is a fingerprint, which manages access to Financial Systems such as BAS and Persal. Personalized security is another most progressive feature of the biometric safety system, to permit only you and the other chosen people whom you have enrolled in the system to access the financial systems. The scanners connected can collect and store loads of fingerprints and restricted access to the systems.

### **1.8 Magnitude of the Problem**

Since KZN Treasury is indirectly serving the whole community of KZN Government Departments, therefore the KZN community will be affected if employees have a negative impression on using the biometrics system. Furthermore, KZN Treasury must know if there is chance that the KZN budget is being stolen on the BAS and Persal without any trace and accountability. National Treasury will be affected because they will also run out of funds for KZN, and there will be no development within KZN, and jobs will be lost. Therefore, this will indirectly affect service delivery in the whole of South Africa. The advantages of using the fingerprint security or identification systems is it reduces the possibility of identity theft. Biometric fingerprint systems improve the security and effectiveness of a company and fingerprints provide a reliable way to track employees.

## **1.9 Research Questions**

The following research questions are supporting this study:

- What were the influencing factors of KZN Provincial Treasury's decision to use biometric security?
- To what extent is the KZN Provincial Treasury using the most secure and latest technology in IT security management?
- What influence does the use of Biometric Security have on work performance at KZN Treasury?
- To what extent has the implementation of Biometric security added value to service delivery at KZN Provincial Treasury?

## **1.10 Research Objectives**

This study aims to:

- To determine the influencing factors of KZN Provincial Treasury's decision to use Biometric security.
- To determine the impact of Government employees using Biometrics in IT Security Management at KZN Treasury.
- To determine the impact of Biometric security on work performance at KZN Provincial Treasury.
- To determine whether the implementation of Biometric security has added value to service delivery.

## **1.11 Significance/importance/contribution of the study**

This study is the first in the KZN Treasury to examine the motives and effects of using Biometrics for IT security control. This study will also look at user satisfaction with the change to Biometrics and factors that led to the decision of KZN Treasury to use Biometrics for IT security control. Therefore, the study will add towards an improved understanding of the wider impact of using Biometrics for IT security control and whether it results in an enhancement of the performance of the public organizations.



### **1.12 Justification of the study**

This study should be conducted since there is a scarcity of prior research studies on the utilization of the Biometrics system as a security control at the KZN Treasury in South Africa. Previous research studies from the literature review have assisted to lay the groundwork for understanding the research problem that is being investigated (Koteswari et al., 2016).

A study of this type will help the management and employees of KZN Treasury to see the benefits of using the biometrics system and what implications it has on their day to day duties. If this study is conducted, the Department will benefit in service delivery because management and employees' attitudes and enthusiasm will improve. They will see the positive impact the biometric system has on them.

### **1.13 Research Methodology**

The research methodology provides the research methodology that must be followed in the study including the description of the population, sample, data collection and data analysis.

Methodology is a set of methods that is used to accomplish a particular activity (Kumar, 2019).

### **1.14 Research Design**

This study will utilize a questionnaire method in order to collect information. This will be employed to establish factors leading to the impact on Government employees of using Biometrics in IT Security Management at KZN Treasury.

Questionnaires are instruments to gather data from participants, consist of a list of questions, with the intention of collecting information from respondents. Since the research study will quantify the employees' perception of using Biometrics for IT security control at the KZN Treasury. It will measure the effectiveness and helpfulness or otherwise of Biometrics. Questionnaires are the most appropriate instrument to be utilized to obtain participants' or respondents' perception (Zhang et al., 2014).

The responses are collected in a formalized manner, using questionnaires which are more impartial than interviews. Gathering information using a questionnaire is comparatively quick. However, in

some circumstances, they can take a little bit longer to design and to apply and analyse. Evidence and information can be gathered from a large selection of individuals.

### **1.15 Research Approach**

A quantitative approach research design has been selected to explore the research problems and related questions. The quantitative approach relies more on characteristics of social behaviour that can be measured, patterned as well as quantified (Rahman et al., 2015). The quantitative approach with a questionnaire is most suited to this study. The research strategy will use various demographics in the classification and quantification of data.

### **1.16 Ethical Considerations**

The ethical standard would be practiced during the research implementation. The researcher acquired authorization from the KZN Treasury HR Director and IT Director to conduct the research. Each participant would be well-regarded with respect by providing allowance to choose whether they want to contribute to this study or not.

Privacy and confidentiality was supported because the researcher informed the participants that the information provided will be used for academic purposes only and not be shared with anyone. The researcher has assured participants that no one's name will be mentioned in this study.

### **1.17 Conclusion**

The implementation of Biometric system has established a secured and efficient alternative to traditional authentication schemes. Biometrics is a technology of determining person's identity in accordance with the physiological traits of an individual.

In this chapter the research background, the evidence of the problem exists, the research problem, the research objectives, research questions have been discussed and the importance of conducting this research. The presentation will be done on the literature review in the following chapter two (2).

## **CHAPTER 2**

### **2.0 LITERATURE REVIEW AND THEORETICAL FRAMEWORK**

#### **2.1 Introduction**

In this chapter a presentation of a literature review regarding the impact of Government Employees using Biometrics at the KZN Provincial Treasury is discussed.

This chapter is an overview of previous studies and knowledge regarding Biometrics as IT security control measurement.

The objective of this literature review is to discover existing knowledge about the topic under the Biometrics Security Technology study. This will assist in being able to determine what is known and unknown about Biometrics Security Technology and the research problem. It will also determine gaps in this area of study and assist with resolving inconsistencies. The literature review will also show other schools of thought on this topic, outline the strengths and weaknesses, as well as discover the theoretical or conceptual frameworks to be used to examine this phenomenon.

The purpose of this study is also to determine whether IT security is being compromised in the departments in order to minimize fraud in Basic Accounting Systems and Persal Systems. The study will determine whether the failure to comply with IT Security Management could compromise data and whether it could be exposed to unauthorized users of the system.

Using Biometrics will assist in improving quality of the work and better service delivery in organisations and minimize fraud (Evans et al., 2015). The feelings of employees in the KZN Treasury regarding biometric security devices cannot be the same. Some regarded biometric security devices as an invasion of their privacy and confidentiality, but Management is grateful for the additional security and the essential responsibility and reliability that this system may provide.

#### **2.2 Security Management in KZN Treasury**

Security management is a systematic, repetitive set of interconnected activities to ensure safe operations and thus reduce the likelihood of risks. KZN Treasury uses the Biometric scanning unit to identify individuals through specific inherent characteristics such as a fingerprint for Security Management.

The Biometrics security system for KZN Treasury has innovative security management features for individuals to gain access to financial systems such as BAS and Persal. Personalized security is another progressive feature of a Biometric safety system; it will only permit chosen employees who have been enrolled in the biometrics system to access those financial systems. The scanners connected collect and store loads of fingerprints and restrict access to the systems.

Layton (2016), stated that Security Management assists organisations to evaluate their security risks and enforce suitable security controls in order to assist in complying with governance requirements, information security regulations and privacy.

According to Hortai (2018), using Biometrics in Security Management is very important as it provides the purpose for granting access in line with the access rights of the authorised users, disallow unauthorized entities from accessing the system and builds a good impression on employees. This is for purposes of security audit or billing, the system can collect information on the accessions made.

### **2.3 Biometrics System**

KZN Treasury provides an important function in implementing and supporting the information systems within the province. Biometric technology improved the security control of systems at KZN Treasury and enabled the tracking of individual physical characteristics for identification in order to prevent identity theft and fraud. Biometrics access guarantees that the ICT networks and support systems are sufficiently secure. Currently, KZN departments are experiencing a huge problem concerning fraud, therefore, Biometric access control has been introduced at KZN departments to enhance access controls in order to reduce fraud.

The Biometrics control also improves the acceptability and accountability pertaining to the BAS and Persal systems. Biometric fingerprinting is used as the gateway to access BAS and Persal Systems within KZN departments. Its availability is critical because users constantly need it to be able to perform their duties on these systems. According to Giesing (2003), biometric identification in an organisation can ensure that only authorised users are granted access to the information kept by the organisation. Haas (2004), states that biometrics uses the distinctive characteristics of an individual to be able to identify that person.

Biometrics is a resolution control to grant entrance to significant systems and delivering non-denial services to all users authorised to access those crucial systems from within the Province of KwaZulu-Natal. The system ensures acceptable access measures are enforced to secure critical systems through the use of Biometric. It prevents from damage or loss of information and unauthorized access and ensures that appropriate non-repudiation measures are enforced. It gives an audit trail of important transactions with the information maintained in a secured and protected database. According to Giesing (2003), an individual can be identified within seconds with the Biometric identification systems and that will lead to improvement of customer service.

The biometrics mechanism prevents fraud and ensures accurate accountability for any fraud conducted. Biometrics allows users to securely authorize transactions (Aithal, 2015). The biometrics authentication aims at identifying information on the user's biometric trait or identity. The goal is to control security and privacy matters that have a serious impact on users' lives, particularly considering the reversibility of biometrics templates and user traceability. Biometrics enables an authorized party to track a user's authentication attempts over different transactions or applications. Results of productive traceability are cross-matching, profiling, and tracking of individuals (Pagnin and Mitrokotsa, 2017). According to Giesing (2003), accurateness identification is important to allow organisations to deliver a better service to their clients and to prevent individuals from distorting themselves to the organisation. The successful and accurate identification, will enhance administrative productivity, keep organisational resource secured.

Fingerprint technology specifically can produce the most reliable and accurate user authentication mechanism. The Biometrics authentication mechanism is a fast progressing mechanism that is concerned with individuals' physiological characteristics identification (Oko and Oruh, 2012).

El-Sayed (2015), declares that performance of biometrics system is measured by the failure of unauthorized users trying to access the system. Each person is unique, they have different physiological characteristics from the other person and that is what the biometrics system uses for identifying an individual. The biometrics system performance is to achieve accuracy, speediness, and other means required by the system. Biometrics system provides acceptability

that the particular user cannot object to his own physiological characteristics. Resistance and avoidance tests provide proof of how the system can resist fraudulent methods easily.

There is an important need to control the users' access to applications and hinder impostors from accessing essential information to use for their own personal benefits. The biometric recognition method was formed based on the facts that each person has unique fingerprints that distinguish them from others (Alsaadi, 2015). Having a user-friendly system is a wise choice to have that will not distract and create difficulty to the users and result in time wastage. Using the fingerprint method to access the system creates confidence and is easy to use for the users (Hortai, 2018).

The type of biometric technology to be used in the university environment is popular considering the quality of individuals that they are dealing with, the easiness of biometric authentication mechanism is used in universities in consideration of security and privacy of people's details. This choice provides an understanding of why the use of biometrics is so important to comprehend and to determine where to use it and how to implement it while keeping in mind the implementation cost implications and maintenance operations.

Biometrics authentication is a technique that is utilised to obtain an individual's identity or verification of a person who claims identification, based on physiological characteristics. This technique is based on the identification patterns that are operated by captured and stored data from an individual's physiological characteristics. Biometrics compares the characteristics captured with the characteristics of the recorded data in the database system (Harinda and Ntagwirumugara, 2015).

According to Alsaadi (2015), the biometric fingerprint authentication system is installed in a mobile phones particularly smartphones and tablet which makes it to be more attractive authentication technique.

Hortai (2018), stated that the biometrics can be used for information exchange between authorised users while making sure that the performed actions are not being declined. Most individuals are more apprehensive with the breach of privacy when using the biometrics system explained (Harinda and Ntagwirumugara, 2015).

Several systems that are developed are making use of biometrics system for individual's identification. The biometrics utilized can be especially appropriate or inappropriate for any given application depending on its specific strengths and weaknesses. A transitory survey was conducted to contrast the different frequently used biometrics methods such as fingerprint, iris and so on outlining the fundamentals of how they work and the inspirations behind the use of each one. The finding was that the biometrics fingerprint method frequently used and easy to use method (Prasanna et al., 2016).

Felkins (2015), identifies the logic received from the scanner over the vehicle network, biometric data for an operator of a vehicle and compares the biometric data from the scanner to sets of biometric data stored in a memory device of the vehicle. It was proven by Felkins (2015), that determining the biometric data from the scanner matches one of the sets of biometric data stored in the memory device, the logic retrieves operational settings configured for the operator and implements at least one action to achieve a result defined by the operational settings.

## **2.4 Different Types of Sectors using Biometrics**

### **2.4.1 Biometrics in Banking**

The banking sector has been working with biometric security technology for identification and authentication. There has been a widespread acceptance of fingerprints for biometric recognition due to numerous influences such as the realistically excellent accuracy, easy to utilize and the minimal capacity of memory space to capture biometrics pattern. According to Haas (2004), the biometric techniques is valuable in possibly solving a list of problems and the most common one is the issue of identity theft. The fingerprint authentication use decreased due to aging or dirty skin of the finger and changes due to cracking (Ananth,2009).

According to Kwakye (2015), "The banking industry is apprehensive with protecting and safeguarding data and privacy of transactions." The biometric technology was adopted as the means of identifying and validating individuals as the solution to the security challenges faced by the banking industry. ATM transaction verification of banking transactions is also using fingerprint identification as one form of biometric authentication.

According to Koteswari et al. (2016), also added his view regarding the ATM verification specifically more on examining of ATM security and the requirement related to biometric identifiers. There is a brief discussion about the materials and techniques developed to direct the impression of Biometrics.

Oye and Nathaniel (2018), stated the current approaches of controlling fraud accomplishments will in no doubt pose incredible problems due to the unpredictability of security influences. However, there is a demand to develop software that will improve the proper control processes of accurate fraud recognition and avoidance in the banking sector.

According to Pradhan (2015), establishing and identifying an individual has become more critical in our heavily interconnected humanity. Therefore, there is a need for reliable user authentication tools that have increased emphasis on concerns with security in networking, communication, and mobility. Pradhan (2015), concluded that it acts as a way of creating identity assisting to secure information and systematize operations in information technology. Biometrics serves as a crucial point to resolve issues relating to personal identification and verification technology.

According to Buciu and Gacsadi (2016), the condition is even more critical with the usage of mobile access where losses due to fraud or identity theft are measured in the hundreds of billions of dollars. Thus, implementing more authentication methods by replacing conventional ways with biometrics for mobile devices seems to be a safe solution (Buciu and Gacsadi, 2016).

Therefore, prevention of fraud has become a critical element in the success of online financial transactions. A biometric authentication system is introduced to improve security for financial transactions. Some measures of security are already part of the authentication mechanism of mobile phones as a mechanism to prevent call theft (Aithal, 2015). According to Lewandowski (2017), the most attractive solution in mobile banking and also solutions applied in branches of the banks is biometrics.



### **2.4.2 Biometrics in E-voting**

Rotich et al. (2017), stated that the E-voting architectures use biometrics to identify and verify a voter. His study investigated biometric properties for identification of insecure e-voting applications for identification that can be used to enhance security. The use of biometrics to identify and verify voters was important to Independent Electoral and Boundaries Commission (IEBC) and to the government in enhancing the use of E-voting to improve transparency. Multi-biometric sources use multiple sources of information for individual authentication which eliminates irregularities in voter identification, vote casting, and vote counting, vote tallies, and auditing. E-voting implementation in developing countries is hindered by the lack of implementation of multi-biometric technologies.

### **2.4.3 Biometrics Attendance Recording system (BARS)**

Biometrics systems also assist by excluding huge files of paper in a manual system and the problematic issues of ghost employees. Its presence provides a crucial method for tracking the attendance of employees in an organization. The olden day methods, where presence was taken and managed manually, were not only troublesome but also inadequate in handling the increasing need for security. Earlier registers and roll calls were utilized for recording signatures of employees on day-to-day activities. Registers have information about employees with an authenticity that could not be verified. Employees could simply tick the presence of another employee. To address this issue, smart cards and card readers were introduced as a solution to prevent an individual to simply sign in and sign out. The issue regarding the cards was that an employee could simply swipe the card of another employee who was absent.

Villaroman et al. (2018), stated that the Local Government Unit (LGU) uses the Biometrics system to deliver an additional widespread technology in observing employee presence and determines that it does not distract service delivery. It provides evaluation influence of the Biometric Attendance Recording System (BARS) use relation to employees' effort routine in regards to Individual Performance Commitment Review (IPCR) score-rating, assessment, and observation. Most employees consider the use of BARS as a way to measure work performance.

The old manual method had gaps allowing an increase in dishonest actions. The Biometrics Attendance Record System (BARS) was implemented to verify employees' attendance by using

both finger and face authentication. Biometrics system validates the individuality and keeps records of entrance and departure intervals with completed particulars of the employee. An instant when an employee uses Biometrics Attendance Record System, the complete particulars are systematically captured in the system. Biometrics is most reliable, secure and does not permit an unauthorized person to utilize. BARS do not allow fraudulent activity as the employee has to mark his attendance in real-time with his physical characteristics. The BARS prevented ghost employees. The Biometrics system is also operative when permitting or rejecting access to restricted areas. It provides help in monitoring security in such cases (Narang et al.).

Villaroman et al. (2018), claims that Biometrics promotes transparency to the organization to save the duration of employees preparation records as the system continuously updating in real time. Implementing BARS saved the organization with several resources which would have been utilised to monitor the attendance of employees, therefore, it creates an increase in work performance.

The organisation uses biometrics system time and attendance clocks for the Human Resource personnel to gain sufficient time in handling employee absences and identifying the ghost employees which means that the use of Biometrics will have a significant impact on their attendance (Villaroman et al., 2018).

#### **2.4.4 Biometrics in Travel**

According to Tock (2015), employees feel that organizations are using biometrics to monitor and track their activities, which is invading their privacy. The biometric technology delivers greater stages of accurateness, safety, and convenience that provides a significant comprehended degree to which it is appropriate also in travel. Morosan (2016), evaluates the enforceability of biometrics technology in travel, highlighting crucial challenges and opportunities. He specifies the opportunities that are provided by biometrics technology in travel systems to provide greater identity management, decreased inconvenience and improved human resource management. The use of biometrics identifiers will provide effective security, especially since an individual will be unable to claim another person's identity or forge travel documentation (Haas, 2004).

Morosan (2016), has identified some opportunities that could be explored through particular biometrics systems, such as immigration systems, traveller programs, identity management systems, biometric passports, hotel access systems, and payment or retail systems. However, he thinks that even though biometrics system is capable of used in travel industry, it is important that the travellers have interest to use or to adopt it.

Biometrics system is utilised to gather biometric data from individuals regarding issuing of identifying documentation, credit cards, identity badges, and documents entitling people to benefits. The system usually congregates evidence information such as fingerprints authentication, facial image authentication, and other biometrics authentication information (Berini et al., 2016).

## **2.5 Features of Biometrics**

Biometrics authentication is a technology of identifying individuals based on physiological characteristics such as face, fingerprints, iris, voice, gait, and signature. A biometrics system may be referred as a blueprint grouping system that uses advanced processing schemes to compare and match biometrics data (Evans et al., 2015). Fingerprint authentication systems have a smaller size, user-friendly or easy to use and consume less power (Faridah et al., 2016). According to Haas (2004), everyone's fingerprints are different and unique, so fingerprints can be accurately recognised and matched. Because the use of fingerprinting has been here ages ago, many people became familiar to use it, but some people have linked the use of fingerprint with criminal stigma.

Faridah et al. (2016), referred to Biometrics as biometrics identification due to the fact that a person can be automatically recognised based on their physiological characteristics, therefore, every person has their own exclusive characteristics that explain their personal identity.

Biometrics systems require that the users make use of some biometric characteristics that can be verified against some stored biometric data. These days, Biometrics-based authentication has become progressively attractive and common for most of the human-computer interaction devices Buciu and Gacsadi (2016). According to Haas (2004), biometrics characteristics function

as a person's password to grant access to the system, they provide uniqueness to the person, can never be forged, or stolen.

According to van Maanen (2016), Biometrics comprises several methods such as facial and voice recognition that can be attributed to at least nine characteristics and encompasses technical, tactical, operational, and strategic processes. The outcome of biometrics provides insight into the biological and biographic identity attributes of individuals and results in Identity Intelligence when fused with situational and reputation intelligence provided by Forensics Enabled Intelligence and Document and Media Exploitation. The biometrics techniques include the face, fingerprint, signature, and iris biometric capture, processing, quality checking and matching identity document collected and tested urged (Berini et al., 2016).

The biometric characteristics are defined as a physiological attribute of humanity that can uniquely identify the individual from another. Currently, the major interest for biometrics authentication systems is justifiable due to greater demand for security. The biometrics main aim is to either provide an automatic verification recognition or recognition of identities, given input data including images, speech or videos. Nelson et al. (2015), claims that the use of biometric identification devices such as cameras for face recognition and profiling, microphones for voice recognition, fingerprints, iris scan, or hand geometry permit highly accurate identification without the use of removable identification devices such as identification badges which may include bar codes, magnetic strips or wireless devices such as RFIDS. However, identification badges are removable and hence susceptible to being lost, misplaced and stolen.

Fingerprint technologies are the earliest in biometrics science and utilize unique characteristics of the fingerprint to recognise or verify the identity of a person. All fingerprints have distinctive patterns and characteristics and an ordinary fingerprint pattern is made up of lines and spaces (Thirumoorthi, 2018). According to Faridah et al. (2016), biological traits such as fingerprints are reliable in performance and much better compared with behavioural traits such as signature, voice or keystroke. It is not easy to decide which authentication technique to implement and utilise in electronic documents and information systems. Harinda and Ntagwirumugara (2015), claimed that the utilisation of hand geometry authentication has been broadly valued and appreciated.

## **2.6 Employees' perceptions in using Biometrics**

Most organizations monitor the employee's activities using biometrics. Organizations have confirmed that using Biometrics provides greater security and improved customers' confidence in the banking sector (Okon and Oruh, 2012).

Villaroman et al. (2018), concluded that most of the employees consider that the utilising of the Biometric Attendance Recording System (BARS) provides an optimistic influence on work performance and the results in using Biometrics confirmed a significant growth in employees' level of performance. According to Giesing (2003), biometrics is accepted by individuals when it adds value to service delivery that will include a security factor and increased accessibility through speed and ease of use.

According to Tock (2015), the investigation of legal and ethical insinuations regarding employee action observing a particular concern specified to influences of system location, ownership of the monitored action and employer motivations in monitoring employee action.

Organizations are failing to comprehend the motives when employees take on or discard new technology. The motive to adopt change with the new technology is not easy for the users and they have no interest in using it, eventually resulting in possible business financial losses. There is an extensive lack of employee participation in implementing of biometric security technology in organizations (Carroll, 2016).

There is an issue that training is needed to use biometrics device appropriately (Kukula and Proctor, 2009). According to Bhagavatula et al. (2015), currently, the use of fingerprint recognition to authenticate had a major positive perception of the scheme's security that influenced employee participation in using Biometrics. User acceptance is a factor that must be considered in the implementation of the biometric system (Kukula and Proctor, 2009).

According to Bhagavatula et al. (2015), users found that adoption of face authentication was absolutely impractical. Using biometrics facial method in a dark area did not work, basically it was only used where there was light for visibility. According to Giesing (2003), users perceive the biometric fingerprint identification system useful, reliable and desirable to use.

Morosan (2016), has also identified some challenges experienced by employees which included confidentiality, fear of damage resultant from utilizing the system, and common user nervousness. According to Giesing (2003), users require to have an assurance that the departments have implemented some proportional measures to be protected from unauthorised users' access to the system.

There has been a major difference between the work performances of the users prior to the implementation and after the implementation of the BARS in Cabanatuan City Government (Villaroman et al., 2018). According to Giesing (2003), the accessibility of biometrics, ease of use and the real time of the verification are important to users. Biometrics enables an unauthorized party to track a user's authentication attempts over different systems (Villaroman et al., 2018).

## **2.7 Training needs**

Like with any other technology that people are unfamiliar with, training is a necessity when the system is introduced for the first time. Giesing (2003), states that when users are supported and trained during their first time use of the biometrics authentication system, this can create an interest to use the system. Training grants users with basic knowledge on the system functionalities and the basic steps for interaction with it. The biometrics systems have similar functions allowing the biometrics training to be the same throughout the entire biometrics systems, enforcing that users do not require any extra training when a new biometrics feature is introduced, for instance if the organization is moving from facial authentication to fingerprint authentication, therefore there will be no training required (Kukula and Proctor, 2009).

## **2.8 Technology Adoption**

New technology can be unpredictable and can create possible negative impacts. Giesing (2003), stating that people tend to use or not use a system until they believe it will help them improve on their job performance or on other hand to perceived usefulness. Technology is a ubiquitous complex system with intellectual features that have a bearing on every aspect of human life. The technology adoption model is in connection with an individual's perceptions and attitudes towards forming part of an adoption process that could have an influence on the user adoption of biometrics as an identification technique (Giesing (2003).

## **2.9 Advantages and Disadvantages**

### **2.9.1 Advantages**

The advantages of using biometrics are related to the characteristics of biometrics. Biometrics relies on the biological characteristics of an individual to uniquely identify a person (van Maanen, 2016). According to Bhagavatula et al. (2015), there are advantages that the users do not have to carry or remember anything such as pin or password.

The security reasons for rolling out fingerprint authentication has been accumulating in several institutions for different purposes because of the ease of use method in comparison to the older methods which used physical inking of individual fingerprint that the users found it difficult to removing the ink later on (Alsaadi, 2015).

Biometrics is more reliable, its traits are persistent and distinctive over time. It also meets some other criteria such as user acceptability and convenience due to privacy motives (Buciu and Gacsadi, 2016). According to Aithal (2015), Biometrics is a secure identification mechanism allowing precise allocation of responsibility for fraud.

### **2.9.2 Disadvantages**

The major threats are potential attacks with fake biometric models. The attackers could use faked biometry for authentication such as an authorised individual's fingerprints model or rubber mask of the imitated face where the biometrics sensor would not be able to differentiate between the copies and the original so the system would successfully authenticate the fraud user (Hortai, 2018).

The Biometrics security levels are not the same and they indicate various types of errors which might provide authentication denial to the biometric sample holders resulting to various factors such as aging, physical damages, cold, weather, etc. (Harinda and Ntagwirumugara, 2015).

Users with dirty hands trying to gain access using biometrics fingerprints method, result in getting their access being denied from the system (Bhagavatula et al., 2015). The biometrics fingerprints authentication has difficulty in gaining good quality images of fingerprint due to the cuts, dirty, wear and tear fingertips (Alsaadi, 2015). Some individuals find it very disturbing to

use fingerprint because they still relate it to criminal identification techniques (Thirumoorthi, 2018).

## **2.10 Theoretical Framework**

The aim of this study is to use the Technology Acceptance Model (TAM) and Delone and Mclean (2004) frameworks to scrutinize employee insights concerning the use of biometric authentication systems that are implemented in ICT. There are diversified biometrics systems that are accessible in the private and public sectors. This study will only emphasise the fingerprint biometrics type and exclude other types such as face recognition, voice recognition, iris scan, or hand geometry. The researcher decided to use two frameworks the Technology Acceptance Model (TAM) and the DeLone and McLean Model. The study focused on the attitude towards using, perceived usefulness and perceived ease of use factors. Focus is only from TAM since other factors are not related to the study and focused on information quality, user satisfaction, individual impact and organization impact from the DeLone and McLean Model, the research found these factors related more to the study being conducted to determine impact of using the Biometrics security technology on employees of the KZN Treasury.

### **2.10.1 The Technology Acceptance Model**

The Technology Acceptance Model (TAM) is an information system (IS) theory describing the manner in which users use and accept the concept of technology. TAM describes factors affecting users when they are offered a new technology. Numerous factors will have an effect on their decisions. There are two underlying factors to the choice to accept the use of technology:

1. Perceived Usefulness
2. Perceived Ease of use

This model gives the provisional explanation to the study on how users come to accept and use a technology (Rahman, 2016).



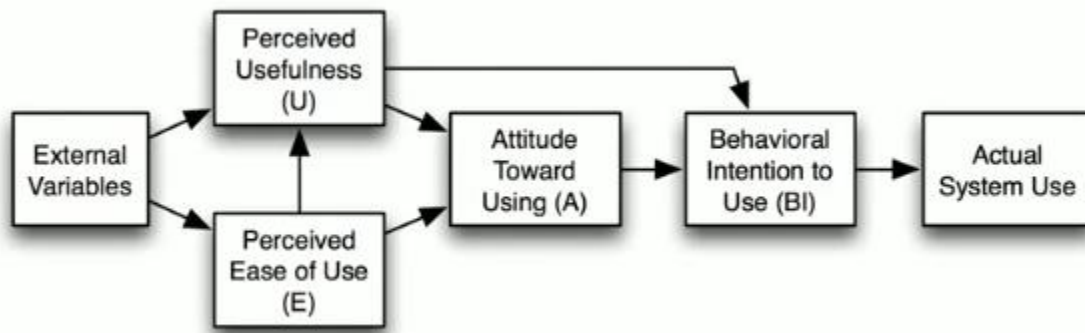


Figure 2.1: The Technology Acceptance Model

### 2.10.2 DeLone and McLean (1992) Model

The classification and collaborating model for identification of indicators that contributed to individual impact on the use of the system and how it is contributing to the organizational impact Delone and Mclean (2004).

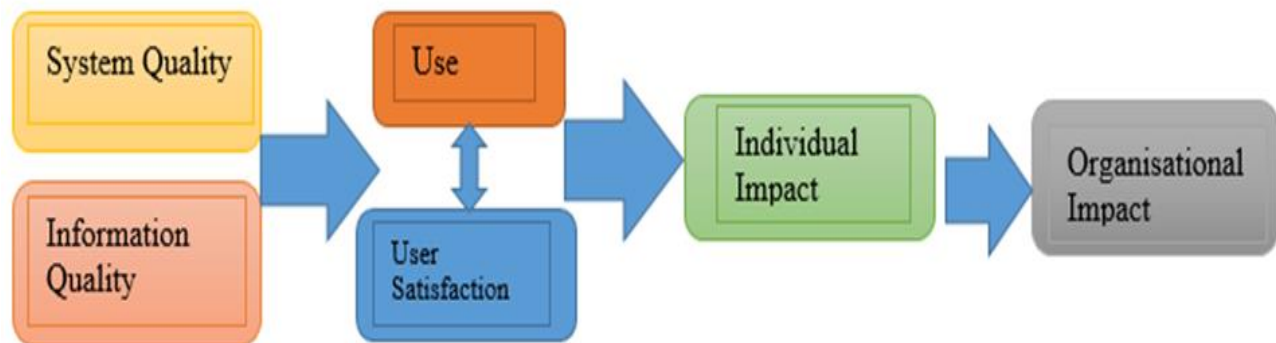


Figure 2.2: The DeLone and McLean (1992) Model

### 2.11 Conclusion

Biometrics has become the more and more common instrument of security improvement. In order to improve security, biometrics fingerprint authentication can be utilised in mobile devices (Aithal, 2015). Users generally considered biometric authentication to be much more secure than PIN codes. The Biometrics systems can be deceived with false fingerprints or a copy of the individual's characteristics but it is can be still be considered as a reliable system (Bhagavatula et al., 2015). Fingerprint recognitions are widely being utilised by banks for ATM accessibility.

This is also more common at grocery stores where it is used to automatically identify recorded customers and bill their accounts (Thirumoorthi, 2018).

The key purpose of implementing biometric systems is to strengthen security. Biometrics provides more secured security features and accessibility than the old methods of using a pin or password. In some other systems, biometrics complement the existing technology and in others, it is a feasible approach. The decision-makers have to understanding of the security level ensured through the use of biometric systems and the differences that exist between the reality and the of the perception sense of security provided. In the next chapter will present the methodology to collect data for analysis in order to achieve the objectives of the study.

## **CHAPTER 3**

### **3.0 RESEARCH METHODOLOGY**

#### **3.1 Introduction**

In this chapter the presentation of the research methodology that is followed for the study including the description of the population, sample, collection of data and data analysis is being discussed. The methodology is a set of methods that are used to accomplish a particular activity.

The aim of this study was to investigate the impact of Government Employees using Biometrics in IT Security Management at the KZN Treasury. The five-point Likert scale questionnaire was developed to gather the relevant data for analysis and interpretation as well as drawing relevant conclusions and recommendations. There was discussion regarding the various aspects related to research methods and techniques that were important in this chapter and the presentation regarding the ability to generate effective results in order to achieve the purpose set by this study.

From many years, information has been gathered in different ways by researchers using various methods such as qualitative, quantitative and mixed methods to come up with resolutions in solving different problems. The researcher decided to use the quantitative method together with data for this study. The privacy and confidentiality policy of the department had to be taken into consideration. The department has a very strict policy for granting access to the employees for conducting research.

#### **3.2 Research Method**

The research methodology categories are namely quantitative and qualitative approaches; however, this research followed the quantitative method and designed questionnaire with responses populated. The quantitative approach relied more on characteristics of social behaviour that can be measured, patterned as well as quantified (Rahman et al., 2015). A quantitative approach with a questionnaire was the most suited to this study. A quantitative approach and research design were selected for this research problem and with related questions. The research strategy used various demographics in the classification and quantification of data.

Quantitative research depends primarily on the collection of quantitative data where the researcher collected data and ensured that it is accurate and fits into rating scales. The researcher felt that the qualitative method will be time-consuming as it involves in-depth interviews, participation observation, field notes and open-ended questions. (Rahman, 2016). Quantitative analytical techniques were utilised to provide interpretations produced by data regarding existing relationships. This study utilised the quantitative approach and design a questionnaire with responses populated and the research strategy emphasised the quantification of the collected and analysed data.

### **3.3 Reasons for selecting this Research Method**

This study was conducted using the quantitative method, there were several views such as the employees' attitudes, opinions, behaviours towards using biometrics and larger sample population to determine the results. All such views, ideas and opinions were considered seriously to this study, to define the most useful results based on what the researcher was searching for, when data is analysed. Using the quantitative method made it easy to analyse data and to provide predictions. Quantitative method assisted the researcher to use measurable data in order to conclude facts and reveal different research patterns. The researcher selected the quantitative method to examine numerical data and use of statistical tools to analyse data collected and represented using graphs and tables. This study is based on Biometrics in IT Security Management, the suitable option was to use a quantitative approach to get many views on the impact of Government Employees using Biometrics in IT Security Management.

### **3.4 Research Design**

A research design is a strategy used in the collection and analysis of variable specified the purpose of addressing the stated research phenomena. This study utilized a questionnaire method in order to collect information. This was employed to establish factors leading to the impact of Government Employees using Biometrics in IT Security Management at the KZN Treasury.

Questionnaires are instruments that were used to gather data from participants, consist of a number of questions, with the objective of collecting information from respondents. Since the research study will quantify the employees' perception towards using Biometrics as the IT security control at KZN Treasury. Therefore, it will measure its effectiveness and helpfulness or lack of

effectiveness and helpfulness. Questionnaires are the most appropriate instrument to be utilized to obtain participants or respondents' perception (Zhang et al., 2014).

The responses are collected in a formalized way, the questionnaires were more impartial, compared to the interviews. Commonly, it is comparatively quicker to gather information using a questionnaire than conducting an interview or case study. However, in some circumstances, questionnaires can take a little bit longer time to design and also to apply and analyse it. Possibly evidence of information can be gathered from a large portion of individuals. The following research questions were to be answered supporting this study:

- What were the influencing factors of KZN Provincial Treasury's decision to use biometric security?
- To what extent is the KZN Provincial Treasury using the most secure and latest technology in IT security management?
- What influence does the use of Biometric Security have on work performance at KZN Treasury?
- To what extent has the implementation of Biometric security added value to service delivery at KZN Provincial Treasury?

### **3.5 Research Methods**

The researcher decided to use one of the classic social sciences research tools which are the questionnaire for the purpose of this study. The questionnaires were distributed among participants and were used as the research instrument. The research methods may be categorised into two broad sets that are known as qualitative and quantitative approaches or both but the researcher has chosen to use the quantitative method. According to Blanche et al. (2006), quantitative methods begin with the classification of known features that are forming a research problem or phenomena. The predetermined classifications of the research are usually discussed in standardised quantitative methods, which results in generalised comparisons of the data sets.

This study followed the quantitative method and design utilising the use of questionnaire with populated responses. The quantitative approach depends primarily on collecting of numerical data where the researcher will analyse and interpret the data collected to ensure that it is accurate and with reliable rating scales. The qualitative research is about the gathering of qualitative data using techniques for instance depth interviews, observations, field notes and open-ended questions.

Quantitative information was gathered using the questionnaire techniques with a sum of twenty three (23) questions with pre-coded responses. The questionnaires were distributed by the researcher through hand delivery and explaining the objective of this study, the use and requested agreement of the respondent to be part of the study.

The usage of pre-coding helped in interpreting and analysing thoroughly pre-coded questions. The researcher has used statistical data analysis tools to analyse the questionnaire responses and provided with meaningful results. This study was limited to KZN Provincial Treasury biometrics users only.

### **3.6 Data Collection and Analysis**

#### **3.6.1 Data Collection**

Quantitative data was gathered utilising the questionnaire approach. There were a total of fifty (60) participants. The participants were put into three groups. The first group of participants consisted of managers from KZN Treasury. There were 5 different managers involved in the study from Basics Accounting System and Persal. The second group of participants consisted of 6 Biometrics enrolment officers. The last group of participants consisted of 49 users, who were part of the biometrics teams.

Biometrics Security Management	5
Biometrics Security Enrolment Officers	6
Biometrics Security Users	49
Total	60

Table 3.1: Number of participants

#### **3.6.2 Data Analysis**

There is a need for having data collection and also to analyse it (De Luca et al., 2015). The data analysis process quantifies objective business information and gives findings of the analysis of the business process or question.

Participants were requested to respond to questions relating to the impact of biometrics on KZN Treasury employees using an appropriate response scale. The nature of responses will allow for specifying the extent of agreement or disagreement. The nature of responses to questions that will be used is as follow (Strongly Agree, Agree, Neutral, Disagree, and Strongly Disagree).

This study will analyse the responses from the participants and gather the information which may aid in the future for analysing the problems or concerns experienced by the participants when it comes to Biometrics. The quantitative methods provide a more precise, measurable and significance test, evade the challenges of numerous comparisons and also increases the statistics of the study, aligns to the research analyses more closely to the way people think (Kukula and Proctor, 2009).

### **3.7 Sampling Strategy**

#### **3.7.1 Probability Sampling**

Probability sampling consists of the likelihood of the known population being selected. The probability sampling method is created from a random selection of the participants and known within a quantitative paradigm. According to Saunders and Rojon (2014), there are differences between the forms of probability sampling which include systematic, stratified random, simple random sampling, multi-stage and cluster. Bryman and Bell (2015), stated that it is very easy to select the participants in the study and it is less costly to conduct the study using with random sampling method.

#### **3.7.2 Non-Probability Sampling**

The non-probability sampling is a method whereby samples are gathered in a technique that does not permit all the individuals in the population to have an equivalent chance of being selected. There are five forms of Non-probability sampling methods which are convenience, sequential sampling, judgemental, quota and snowball sampling can be used to conduct a study.

For the objective of this study, the researcher had to conduct the study based on the three (3) different groups of participants. The researcher used a stratified sampling method in order to

conduct this study. The reason the researcher selected this stratified sampling method because it allowed the population to be arranged into groups. Therefore, ensured that participants from each group were being represented in the sample. The participants were selected based on specific criteria, such as the system they use with Biometrics implemented as a security control.

The targeted population are the employees of KZN Treasury that are using biometrics for Basics Accounting System and Persal. There are currently 76 employees at KZN Treasury that are using biometrics system.

The researcher targeted three groups, the one group of participants consisted of Managers classification from the Department of Treasury. A total number of five (5) managers were involved in the study from Basics Accounting System and Persal were consulted in order to reach the targeted population. The researcher tried to form a diverse sample as possible, ensuring an equal number in gender (men and women) representation, and more importantly that the various systems had representatives on use biometrics systems such as Basics Accounting System and Persal. The second group of participants consisted of forty-nine (49) users, who were part of the biometrics teams. The last group of participants consisted of six (6) enrolment officers, who were part of the biometrics teams. The sample size of the population was suitable for the purposes of this study as each participant had to complete an individual questionnaire. Each participant was approached, and the questionnaires were hand delivered, then completed by the participants and sent back via hand delivery again. This occurred in the duration of four weeks.

The questionnaires would be sent as follows:

Biometrics Security Management	5
Biometrics Security Enrolment Officers	6
Biometrics Security Users	49
<b>Total</b>	<b>60</b>

Table 3.2: Total number of participants

### 3.7.3 Sampling Technique

Sampling is the statistical method of electing a sample of a population of interest for the aim of conducting a study and statistical inference of that population (Harinda and Ntagwirumugara,



2015). Selecting of sampling methods and determining sample size is extremely significant in useful statistics research problems to provide the correct conclusions (Dunn et al., 2011).

This study was limited to the KZN Treasury employees that are involved in Biometrics security management. The sampling technique that was used in this study is stratified sampling as a form of probability sampling. In this study, there was a separation of people into groups according to some characteristics of their positions in Biometrics. Groups' classification will be as follows:

Management			Biometrics Enrolment Officer	Biometrics Users
Senior Manager	Deputy Manager	Assistant Manager		

Table 1.3: Group classification

The sample size determination is a challenging process to handle stated (Rahman et al. 2015). It is critically important aspect of the study to determine the appropriate sample size to answer the research question.

### 3.8 Instrument Design

#### 3.8.1 Questionnaires

The research decided on using the questionnaires for this study because of the reliability and fastest way to collect information from several respondents in an efficient and less time-consuming. The questionnaires were the only solution for the research to be able to reach multiple respondents within four weeks. A common disadvantage of the questionnaires is that they are unchangeable and has a strict format, which reduces the possibility for more in-depth or abstract observation (Bryman and Bell, 2015). The questionnaires provided linear and clear results.

For this study purposes, the researcher constructed questionnaire scripts. The questionnaire consisted of twenty-three (23) closed-ended questions, related to the impact of employees using biometrics. The first session of the questionnaire contained demographic questions, related to the gender, qualifications, and questions related to the professional role of the respondents in

Biometrics. The main questions were separated into groups for clarity, addressing the objectives of the study. More importantly, these questions were considered to address and established the impact of employees using biometrics as security management control.

### **3.9 Data Collection**

Quantitative factual data was gathered utilising the questionnaire approach. There was a total of sixty (60) participants. This method quantified tendencies following patterns and strategies to identify the correlation between the variables and defined the worthiness of the investment. Most of the communication with the participants occurred face to face. The researcher purposely targeted KZN Treasury, because the chances of being granted access to employees were much higher, and the process was going to be less time-consuming, which turned out to be the case. At the beginning the researcher communicated with the relevant employees from units via the phone, to make them acquainted with the purposes of the study. The researcher requested for authorisation to conduct the study with representatives from Basics Accounting System and Persal units. For privacy and confidentiality, the job titles and names of the participants were not revealed, especially because their job titles and their names were not relevant to the study. In some cases, the managers distributed the questionnaires to the employees, and in other cases, the researcher delivered the questionnaire to the employees directly, face to face. The questionnaires were distributed and finalised during the course of four weeks.

### **3.10 Methods of Data Analysis**

There is a need for having data collection and also to analyse it (De Luca et al., 2016). The data analysis process quantifies objective business information and gave findings of the analysis of the business process or in question.

Participants were requested to respond to questions using an appropriate response scale because this study aimed to determine the impact of employees in using Biometrics. The nature of responses was to allow for specifying their level of agreement or disagreement. The nature of responses to questions that were used is as follows (Strongly Agree, Agree, Neutral, Disagree, and Strongly Disagree).

This study obtained the responses from the participants and gathered the entire possible information which may be utilised for analysing the problems or concerns experienced by the participants. The analysis of the questionnaire results took place via statistical analysis. Data Analysis was done using the different forms and answer sets of the questions, and the quantitative approach, the researcher used statistical software available such as SPSS and excel. The outcomes from the questionnaires were demonstrated in the form of tables and charts. The most important findings of this study will be discussed in detail in the next chapter.

### **3.11 Ethical Considerations**

The researcher had to take into consideration several types of ethical issues for this study. The major one related to the informed consent of the participants. The participants (both managers and employees) were informed earlier about the objectives of this study and they gave their informed consent to participate in writing. Their identity details and the name of the section (for instance human resources, financial reporting) that the participants belong to was strictly confidential, thus complying with the requirements of the code of ethics of the University of KwaZulu-Natal.

In addition, the privacy and confidentiality policy of the department had to be considered as well, as the department has a very tight policy for granting access to the employees for research study purposes. Therefore, the researcher signed consent forms for confidentiality and privacy with the Department (KZN Treasury) whose employees and managers agreed to participate in the study.

Lastly, all the information received in the course of this study will be used only for the purposes of the research and will remain confidential. The ethical standard would be practiced during the research implementation. The researcher acquired authorization from the KZN Treasury HR Director and Head of Department (HOD) to conduct the research. Each participant was regarded with respect by providing allowance to decide whether they want to contribute to this study or not. Privacy and confidentiality were supported by providing advice to the participants on the questionnaire that they have a right not to reveal certain information to the public. Participants remained anonymous and no names mentioned in this study.

### **3.12 Problems and Limitations**

The researcher encountered several problems and challenges while conducting the research for this study.

The foremost challenge was to recruit an appropriate number of participants. The identification of the potential participants took a long time, and several times the requests of the researcher were not approved, because most of the users were extremely busy with their day to day functions to allow the opportunity for the research. Thus, access to the participants and obtaining permission to conduct the research was a major challenge.

Furthermore, the researcher had limited time to engage with the users, enrolment officers and management. Then the researcher had to determine the choice that will provide a more efficient and effective method, such as the questionnaire, instead of the more time-consuming methods such as the focus groups or participant observation.

### **3.13 Conclusion**

This chapter has provided a discussion on the research methodology implemented in this study and its validity. Because of the nature of this study, the researcher chose to use the quantitative strategy. The main research tools used were questionnaires with three groups of participants the enrolment officers, users and managers. The participants were carefully selected through a stratified sampling technique. The outcome or results were analysed using SPSS and excel, because of the quantity sample of participants. The main results and findings of this study are discussed in the following chapter four (4).

## **CHAPTER 4**

### **4.0 DATA ANALYSIS AND INTERPRETATION**

#### **4.1 Introduction**

The purpose of this chapter is to present the analyses of the responses of the participants. The researcher analysed the responses of the participants collect findings that will establish in the data analysis and provide an advanced review. Data responses were presented from the responses received to provide analysis and interpretations on the impact of Government Employees using Biometrics in IT Security Management at KZN Treasury.

The previous chapter dealt with the research methodology implemented for this particular study. The data collection method that was used was a five-scale questionnaire with response items that are ranging from 1 - Strongly Agree, 2 – Agree, 3 – Neutral, 4 – Disagree, 5 - Strongly Disagree. There are 60 participants that provided responses to the study. The questionnaires were distributed to the enrolment offices, the management and users that are within the department of KwaZulu-Natal Treasury. This chapter also provides an analysis of the data, which facilitates the drawing and graphs for providing the conclusion and recommendations.

#### **4.2 Sample Characteristics**

A total of twenty-three (23) questions were distributed. The researcher received 60 respondents who were willing to participate and completely answered all questions, which made it easier for the researcher not to reject any questionnaire.

#### **4.3 SECTION A: Demographic profile of respondents**

The demographics of the participants were looked into were in relation to the gender, highest academic qualification and current employment position.

##### **4.3.1 Gender of the respondents**

The respondents were questioned about their gender and the table and the chart displays the gender of the respondents:

	FREQUENCY	PERCENTAGE
Female	32	53.3
Male	28	46.7
Total	60	100.0

Table 2.1 Gender frequency

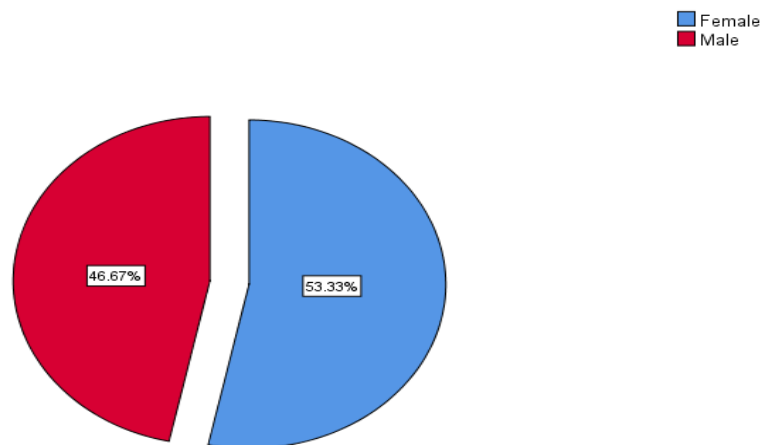


Figure 4.1: Gender

Table 4.1 and Figure 4.1 represent the gender analysis of the respondents' highest rate from females and males. It indicates that females were 53.33% (n= 32) and males were 46.67% (n = 28), therefore this shows that they were more females than males employees using biometrics. The percentage is proportionate to the ratio as females constituted the majority within the Department although there were imbalances with regards to the management positions which are dominated by males.

#### 4.3.2 Current Employment Position

The respondents were asked about the current employment position they are in, Table and chart below depicts the employee's position:

	FREQUENCY	PERCENTAGE
User	48	80.0
Enrolment Officer	6	10.0
Management	6	10.0
Total	60	100.0

Table 4.2: Employment position frequency

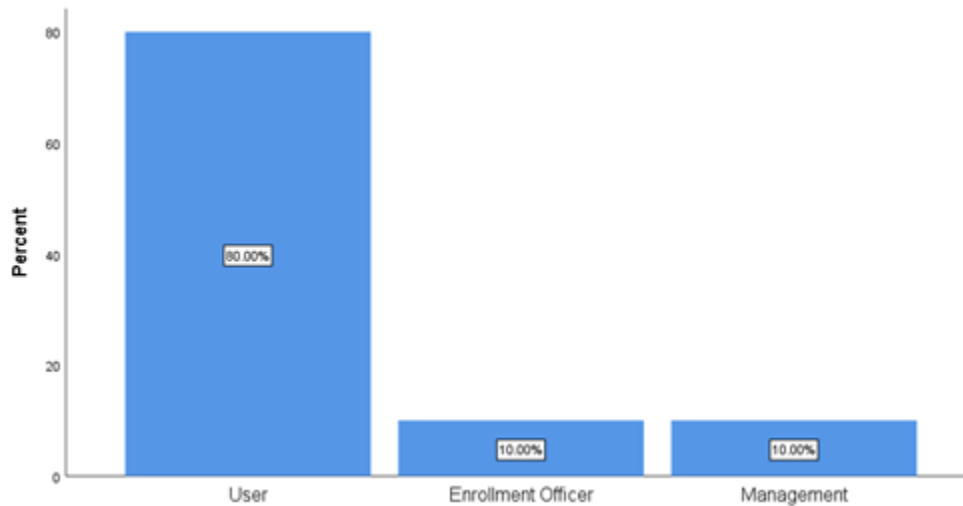


Figure 3.2: Employment Position

The participants' responses in terms of this category shown in Table 4.2 and Figure 4.2. The study indicates that the highest number of respondents were users with 80.0% (n = 48) and an equal number of enrolment officers of 10.0% (n = 6) and management 10.0% (n=6). This indicated that the majority of employees who are using Biometrics at the KZN treasury were users.

#### 4.3.3. Qualification

The respondents were asked about the qualification they possess, the table and the chart below depicts the qualifications.

	FREQUENCY	PERCENTAGE
<b>Matric</b>	<b>2</b>	<b>3.3</b>
<b>National Diploma</b>	<b>35</b>	<b>58.3</b>
<b>Bachelor degree</b>	<b>16</b>	<b>26.7</b>
<b>Post grad</b>	<b>7</b>	<b>11.7</b>
<b>Total</b>	<b>60</b>	<b>100.0</b>

Table 4.3: Qualification frequency

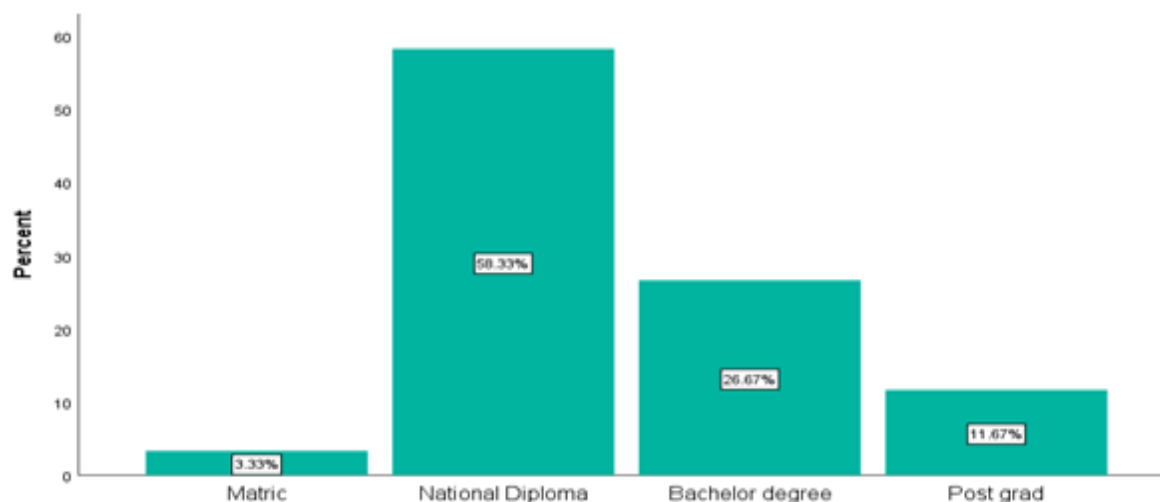


Figure 4.3: Qualification

Table 4.3 and Figure 4.3 above indicate the qualifications obtained by the participants provided who the responses. It illustrated that the majority of employees who provided responses to using Biometrics in the IT security management at KZN treasury have national diplomas 58.3 % (n =35), with bachelor's degree was 26.7% (n = 16), with post-graduation qualification was 11.7% (n=7) and those who have matric were the smallest number of employees with 3.3% (n=2). This shows that employees and the employer is comfortable with having a national diploma in order to do the work required.

#### 4.3.4 Gender by the highest qualification

This tabularisation was used to examine the relationship between variables selected, table 4.4 and chart 4.4 depicts relationships:



GENDER BY* QUALIFICATION						
		What is your Qualification?				Total
		Matric	National Diploma	Bachelor degree	Post grad	
What is your gender?	Female	2	21	6	3	32
	Male	0	14	10	4	28
Total		2	35	16	7	60

Table 4.4: Gender highest qualification

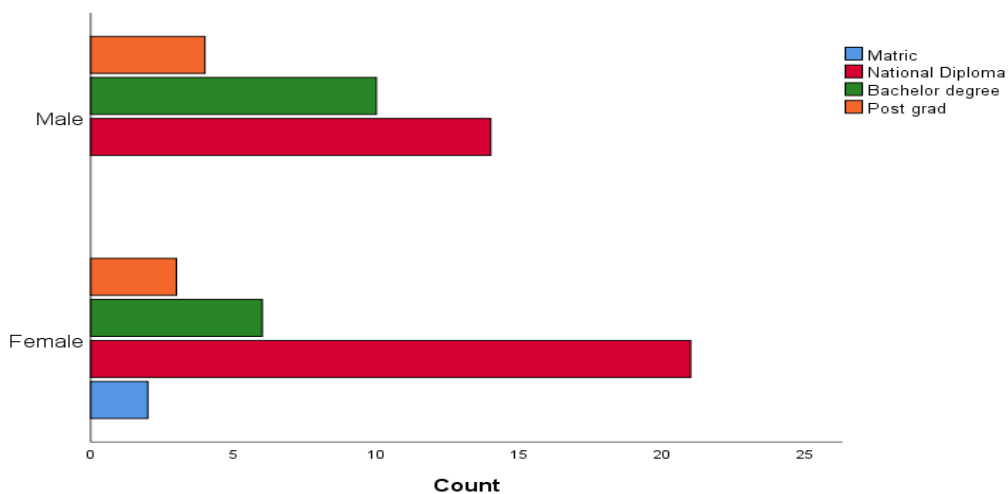


Figure 4.4: Gender highest Qualification

Table 4.4 and Figure 4.4 indicate the genders' highest qualifications obtained by the participants provided the responses. It illustrated that there were more females 35% (n=21) with national diplomas whereas 23% (n= 14) were males. There were fewer females 10% (n= 6) compare to males 17% (n=10) with bachelor's degrees. There were 5% (n=3) females with post-graduate degrees and 7% (n= 4) males. 3% (n= 2) were females with matric and there were no males with the matric qualification only.

#### 4.3.5 Gender by the position in the organization

This table was used to examine the relationship between variables selected, table 4.5 and chart 4.5 depicts relationships:

GENDER* BY POSITION					
		What is your position in the organization			Total
		User	Enrolment Officer	Management	
What is your gender?	Female	29	1	2	32
	Male	19	5	4	28
Total		48	6	6	60

Table 4.5: Gender and Position

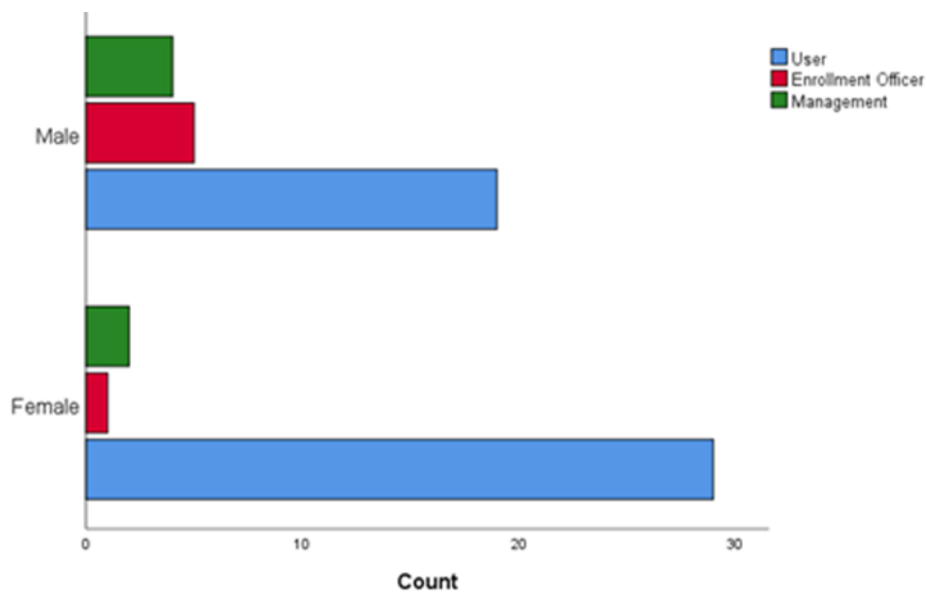


Figure 4.5 Gender and Position

Table 4.5 and Figure 4.5 indicate the positions that the gender occupied by the participants provided the responses. It illustrated that there were more females 48 % (n=29) that are users whereas 32% (n= 19) were males. There were fewer females 2% (n= 1) compare to males 8%

(n=5) were enrolment officers. There were 7% (n=4) males and 7% (n = 4) females. 3% (n= 2) were females in management.

#### 4.4 SECTION B: Perceived Usefulness of Biometrics in System and Information Quality

**Section B** of the questionnaire was designed to define the impact of biometric security on work performance at the KZN treasury and also to clarify the influence that the use of biometrics security has on work performance at the KZN treasury. The frequencies are presented both numerically and in a percentage, format to reflect the respondents' responses which are further illustrated by using bar charts to facilitate data analysis

The numerical values of 1= SA, 2=A, 3=N, 4=D, 5=SD which respectively represent strongly agree, agree, neutral, disagree and strongly disagree are used to illustrate the difference in responses of respondents.

Questions	Total	Strongly Agree (%)	Agree (%)	Neutral (%)	Disagree (%)	Strongly Disagree (%)	Total (%)
Question 4	60	32%	43%	12%	10%	3%	100%
Question 5	60	38%	43%	12%	7%	0%	100%
Question 6	60	55%	27%	10%	2%	7%	100%
Question 7	60	40%	38%	12%	8%	2%	100%
Question 8	60	33%	42%	13%	7%	5%	100%

Table 4.6: Summary of question responses in section B

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	19	31.7	31.7	31.7
	Agree	26	43.3	43.3	75.0
	Neutral	7	11.7	11.7	86.7
	Disagree	6	10.0	10.0	96.7
	Strongly Disagree	2	3.3	3.3	100.0
	Total	60	100.0	100.0	

Table 4.7: Biometrics improves quality of work

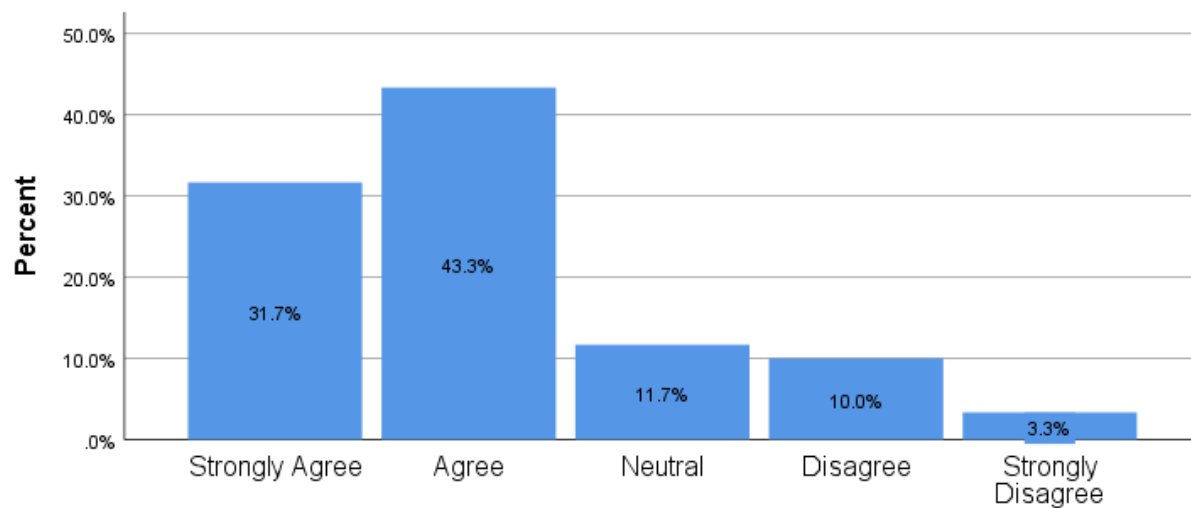


Figure 4.6: Biometrics improves the quality of work

As shown in Table 4.7 and Figure 4.6, approximately 31.7% of respondents strongly agreed and 43.3% agreed that using Biometrics improved the quality of work that is done. The 11.7% was neutral therefore this shows that these employees neither agree nor disagree or are unsure whether the quality of work has improved due to Biometrics. 10.0% disagree and 3.3% strongly disagreed that by implementing Biometrics, the quality of work has improved. This clearly proves that by implementing Biometrics the quality of work has improved as most employees (75%) have agreed. There has been a significant difference between the work performances of the users prior to the implementation and after the implementation of the BARS in Cabanatuan City Government (Villaroman et al., 2018).

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	23	38.3	38.3	38.3
	Agree	26	43.3	43.3	81.7
	Neutral	7	11.7	11.7	93.3
	Disagree	4	6.7	6.7	100.0
	Total	60	100.0	100.0	

Table 4.8: Biometrics provides greater control over the work

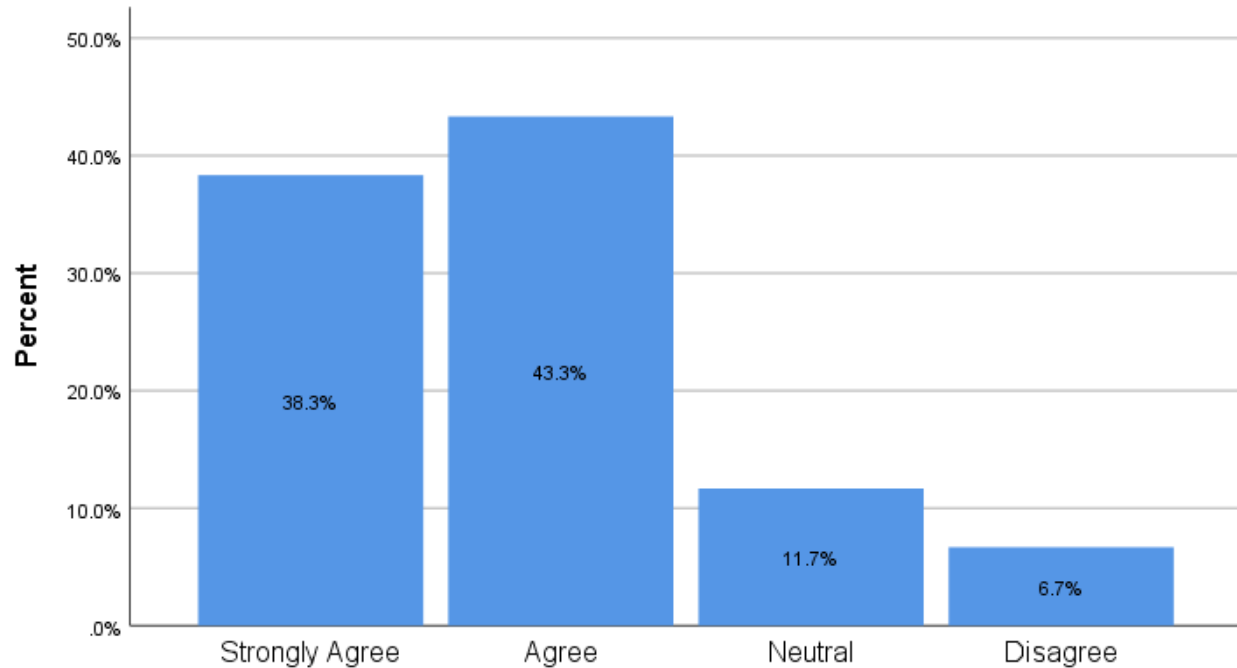


Figure 4.7: Biometrics provides greater control over the work

As shown in Table 4.8 and Figure 4.7, approximately 38.3% of respondents strongly agreed and 43.3% agreed that by using Biometrics, there was greater control over their work. 11.7% was neutral therefore this shows that these employees neither agree nor disagree or are unsure whether or not Biometrics provides greater control over their work. 6.7% disagreed that by implementing Biometrics they have greater control over their work. This question clearly proves that using Biometrics provides greater control over the employees' work as most employees (81.6%) have agreed. (Villaroman et al., 2018) concluded that most of the employees consider that the utilising of the Biometric Attendance Recording System (BARS) provides an optimistic influence on work performance and the results in using Biometrics confirmed a significant growth in employees' level of performance.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	33	55.0	55.0	55.0
	Agree	16	26.7	26.7	81.7
	Neutral	6	10.0	10.0	91.7
	Disagree	1	1.7	1.7	93.3
	Strongly Disagree	4	6.7	6.7	100.0
	Total	60	100.0	100.0	

Table 4.9: Biometrics enables system security control

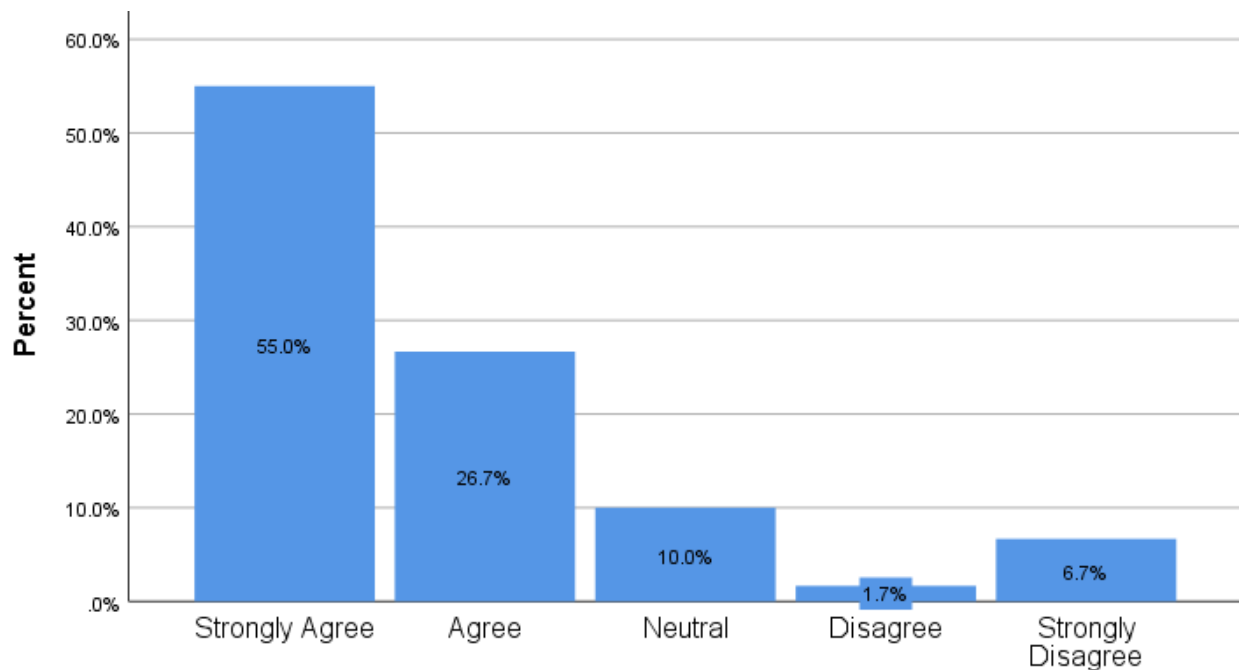


Figure 4.8: Biometrics enables system security control

As shown in Table 4.9 and Figure 4.8, 55.0% of respondents strongly agreed and 26.7% agreed that Biometrics enables system security control. The 10% that was neutral therefore shows that these employees are neither agree nor disagree or are unsure whether Biometrics enables system security control or not. The study indicates that of all the respondents, only 1.7% disagree and 6.7% strongly disagreed that Biometrics enables system security control. This obviously proves that by Biometrics enables system security control as most employees (81.7%) have agreed. Biometrics confirms greater security and improved customers' confidence in the banking sector (Oko and Oruh, 2012).

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	24	40.0	40.0	40.0
	Agree	23	38.3	38.3	78.3
	Neutral	7	11.7	11.7	90.0
	Disagree	5	8.3	8.3	98.3
	Strongly Disagree	1	1.7	1.7	100.0
	Total	60	100.0	100.0	

Table 4.10: Biometrics provides a greater organizational impact

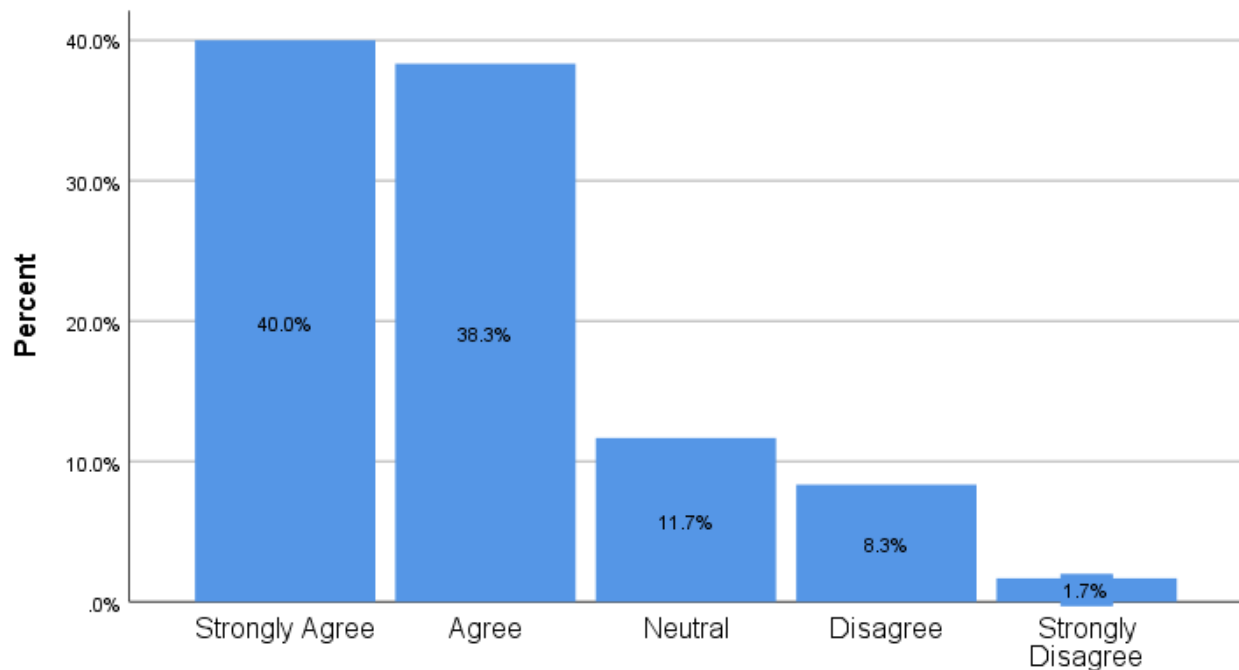


Figure 4.9: Biometrics provides a greater organizational impact

Table 4.10 and Figure 4.9, about 40.0% of respondents strongly agreed and around 38.3% agreed that Biometrics provides a greater organizational impact. The almost 11.7% that was neutral therefore shows that these employees neither agree nor disagree or are unsure whether Biometrics created a greater organizational impact or not. The study indicates that approximately 8.3% of respondents disagree and 1.7% strongly disagreed that Biometrics provides a greater organizational impact on government employees around KZN. This seriously guarantees that Biometrics provides a greater organizational impact on the government employees as most employees (78.3%) have agreed. Layton (2016), stated that Security Management assists organisations to evaluate their security risks and enforce suitable security controls in order to assist in complying with governance requirements, information security regulations and privacy.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	20	33.3	33.3	33.3
	Agree	25	41.7	41.7	75.0
	Neutral	8	13.3	13.3	88.3
	Disagree	4	6.7	6.7	95.0
	Strongly Disagree	3	5.0	5.0	100.0
	Total	60	100.0	100.0	

Table 4.11: Biometrics provides accurate information

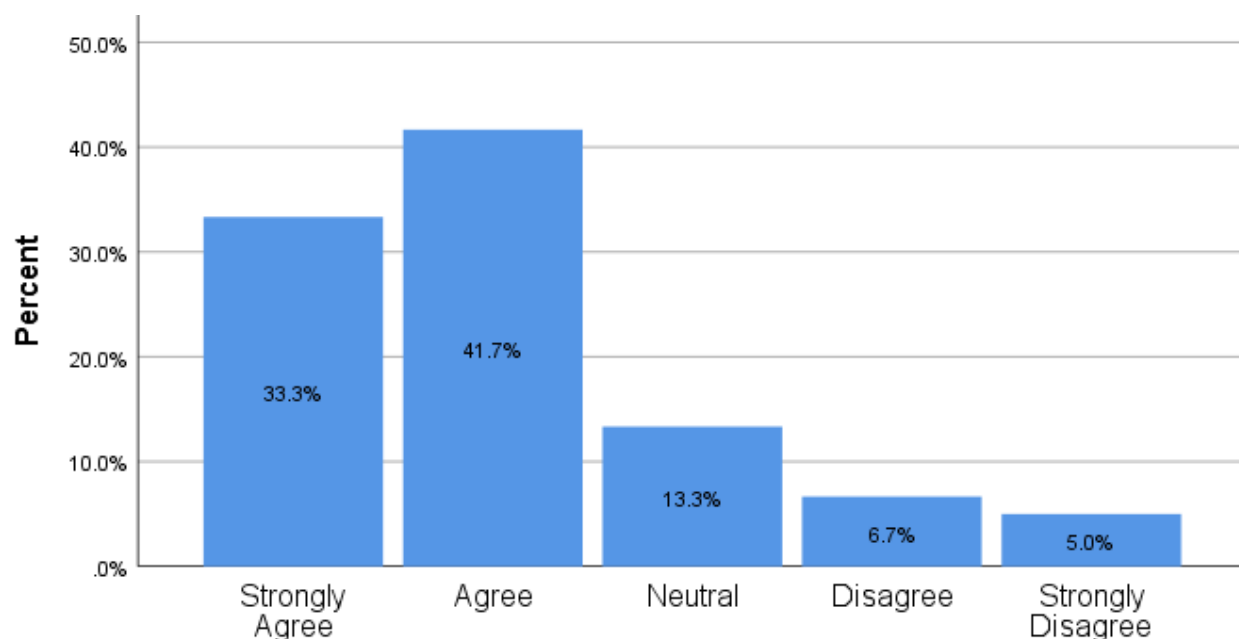


Figure 4.10: Biometrics provides accurate information

Table 4.11 and Figure 4.10, shows that about 33.3% of respondents strongly agreed and around 41.7% agreed that Biometrics provides accurate information. 13.3% was neutral showing that these employees neither agree nor disagree or are unsure whether Biometrics provides accurate information or not. The study indicates that the number of almost 12% of respondents disagreed that Biometrics provides accurate information on BAS and Persal to the government employees around KZN, 6.7% just disagreed and 5.0% strongly disagreed. This study seriously guarantees that by that Biometrics delivers accurate information regarding the financial systems as most employees (75%) have agreed. Villaroman et al. (2018), claims that Biometrics promotes



transparency to the organization to save time in preparation of employee records as the system keeps on updating in real time.

#### **4.5 SECTION C: Perceived Ease of Use of Biometrics, User Satisfaction and Individual and Organization Impact.**

Section C of the questionnaire was designed to verify the ease of use of biometric fingerprinting. This by verifying user satisfaction regarding implementation of biometrics security, whether it added value to service delivery at the KZN provincial treasury, and to clarify the individual and organizational influence that the use of biometric security has on the employees' work performance at KZN treasury. The frequencies are presented both numerically and in a percentage, format to reflect the respondents' responses which are further illustrated by using bar charts to facilitate data analysis.

The numerical values of 1= SA, 2=A, 3=N, 4=D, 5=SD which respectively represent strongly agree, agree, neutral, disagree and strongly disagree are used to illustrate the difference in responses of respondents. The tables 4.12 provides a numeric summary of the participants' responses with regards to the question asked in the questionnaire:

<b>Questions</b>	<b>Total</b>	<b>Strongly Agree (%)</b>	<b>Agree (%)</b>	<b>Neutral (%)</b>	<b>Disagree (%)</b>	<b>Strongly Disagree (%)</b>	<b>Total (%)</b>
Question 9	<b>60</b>	55%	28%	3%	5%	8%	<b>100%</b>
Question 10	<b>60</b>	7%	13%	32%	30%	18%	<b>100%</b>
Question 11	<b>60</b>	47%	35%	10%	7%	2%	<b>100%</b>
Question 12	<b>60</b>	13%	30%	30%	23%	3%	<b>100%</b>
Question 13	<b>60</b>	62%	25%	2%	5%	7%	<b>100%</b>

Table 4.12 Summary of question responses in section C

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	33	55.0	55.0	55.0
	Agree	17	28.3	28.3	83.3
	Neutral	2	3.3	3.3	86.7
	Disagree	3	5.0	5.0	91.7
	Strongly Disagree	5	8.3	8.3	100.0
	Total	60	100.0	100.0	

Table 4.13: Ease of use of biometrics fingerprint as security measure

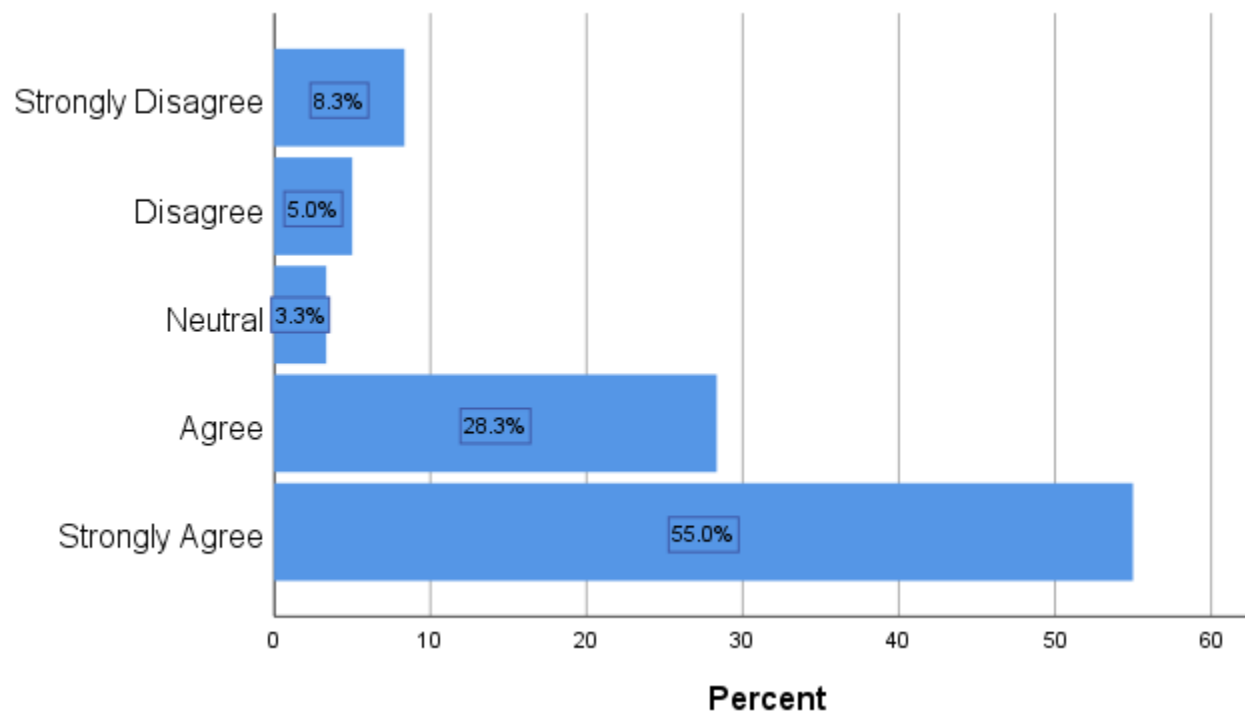


Figure 4.11: Ease of use of biometrics fingerprint as security measure

The Table 4.13 and Figure 4.11, shows that 55.0% of respondents strongly agreed and about 28.3% agreed that they prefer to use Biometrics fingerprint as a security management measure rather than using other Biometrics features like facial, palm, and iris and so on. The 3.3% that was neutral therefore means that these employees neither agree nor disagree or are unsure or they are not familiar with other Biometric features besides the fingerprint. The study indicates that of all respondents, approximately 5.0% disagreed and approximately 8.3% strongly disagreed. This could mean that these employees would prefer to use other Biometric features rather than using the biometric fingerprint or they don't trust fingerprints for security verification. This seriously

guarantees that Biometrics fingerprints as security management measure are the most preferred feature to be used by employees as the most employees (83.3%) have agreed. Using the fingerprint method to access the system creates confidence and is easy to use for the users (Hortai, 2018).

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	4	6.7	6.7	6.7
	Agree	8	13.3	13.3	20.0
	Neutral	19	31.7	31.7	51.7
	Disagree	18	30.0	30.0	81.7
	Strongly Disagree	11	18.3	18.3	100.0
	Total	60	100.0	100.0	

Table 4.14: Biometrics as an unnecessarily complex

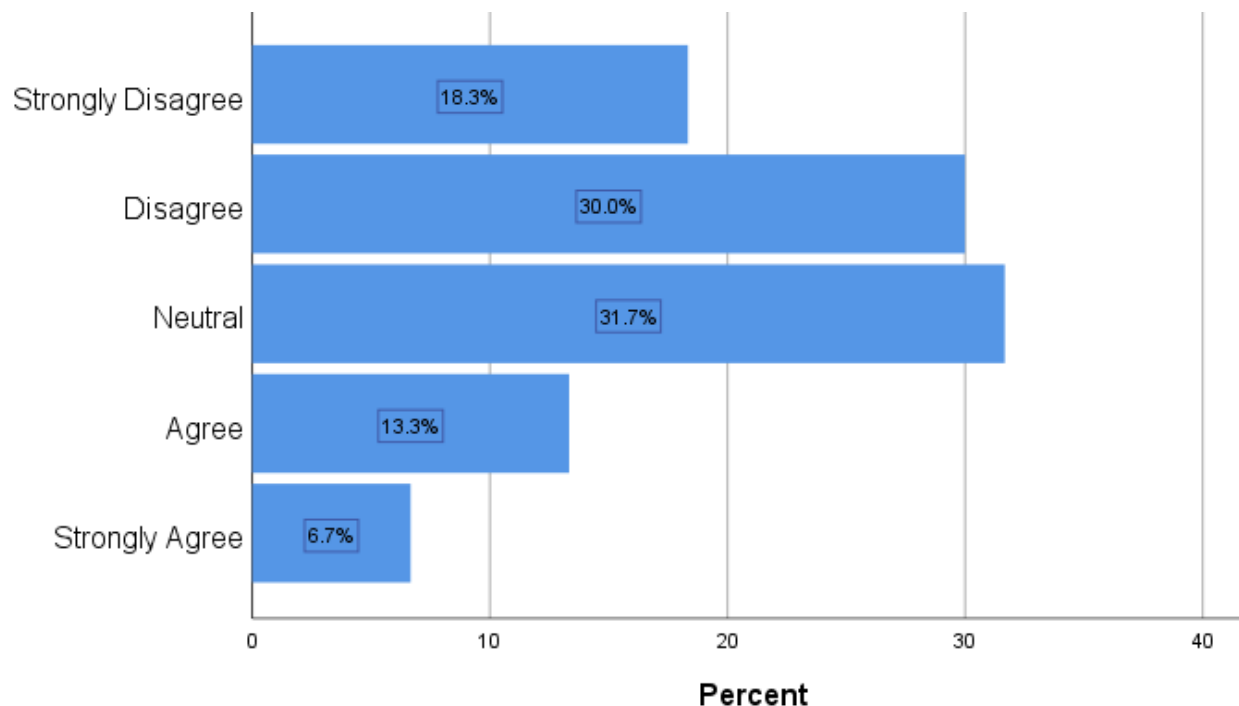


Figure 4.12: Biometrics as an unnecessarily complex

The Table 4.14 and Figure 4.12, demonstrates that 6.7% of respondents strongly agreed and about 13.3% agreed that Biometrics as an unnecessarily complex or feature to use. Therefore, this 20 % would prefer not to use it as an additional feature to gain access to the financial system. The 31.7% was neutral showing that these employees neither agree nor disagree or are unsure about Biometrics complexity or they did not understand the question. The study indicates that

most respondents either disagreed (30.0%) or strongly disagreed (18.3%) that Biometrics is unnecessarily complex. This confirms that these employees feel that biometrics is a necessary feature to be added as an additional log in access. According to Pradhan (2015), establishing and identifying an individual has become more critical in our heavily interconnected humanity.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	28	46.7	46.7	46.7
	Agree	21	35.0	35.0	81.7
	Neutral	6	10.0	10.0	91.7
	Disagree	4	6.7	6.7	98.3
	Strongly Disagree	1	1.7	1.7	100.0
	Total	60	100.0	100.0	

Table 4.15: Easy use of Biometrics System

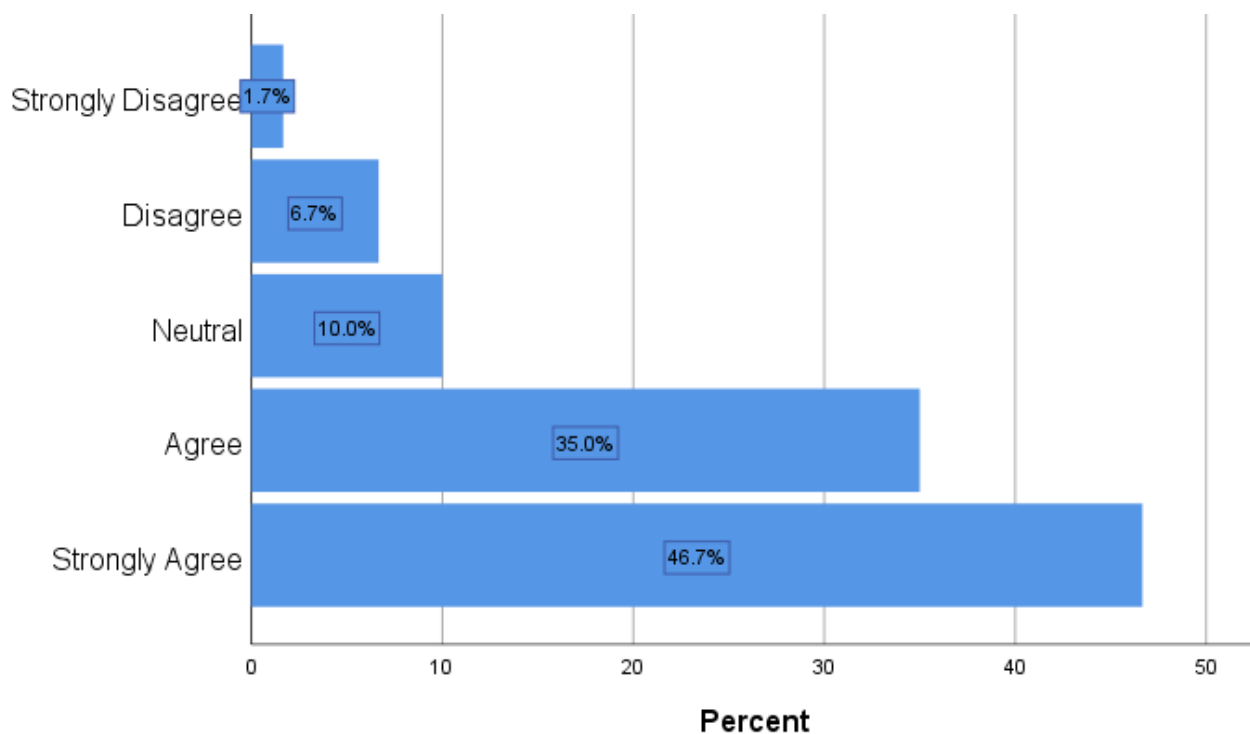


Figure 4.13: Easy use of biometrics System

The Table 4.15 and Figure 4.13, indicates that about 46.7% of respondents strongly agreed and 35.0% agreed that the Biometrics system is easy to use. The 10.0% that were neutral are either not sure or they were not using the Biometrics system often enough to comment. The study

indicates that the number of negative respondents was approximately 6.7% disagreeing and almost 1.7% strongly disagree. This seriously guarantees that the Biometrics fingerprint system is easy to use as the most employees (81.7%) agreed. Fingerprint authentication systems have a smaller size, user-friendly or easy to use and consume less power (Faridah et al., 2016).

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	8	13.3	13.3	13.3
	Agree	18	30.0	30.0	43.3
	Neutral	18	30.0	30.0	73.3
	Disagree	14	23.3	23.3	96.7
	Strongly Disagree	2	3.3	3.3	100.0
	Total	60	100.0	100.0	

Table 4.16: Biometrics as a monitoring and tracking tool rather than security tool

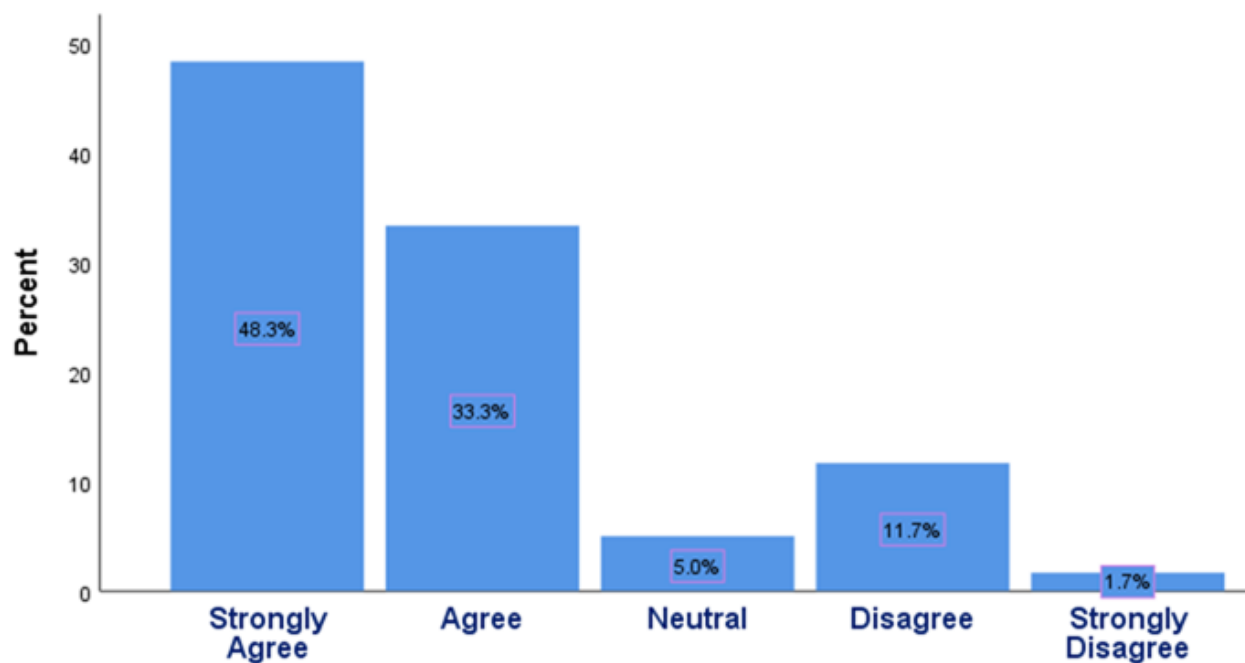


Figure 4.14: Biometrics as a monitoring and tracking tool rather than a security tool

The demonstrated Table 4.16 and Figure 4.14, specifies that about 48.3% of respondents strongly agreed and 33.3% agreed that Biometrics is a monitoring tool and tracking tool rather than providing security for the system. Only 5.0% was neutral therefore this shows that most employees were unsure of their response with a few possibly scared to express their feelings regarding Biometrics. The study indicates that the number of respondents was users

approximately 11.7% disagree and 1.7% strongly disagreed. In this regard, the research will confirm that the employees think that the Biometrics system is mainly implemented to monitor and track them in their duties as most employees (81.6%) have agreed. For some people, it is very intrusive to use fingerprint because they still relate it to criminal identification techniques (Thirumoorthi, 2018).

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	37	61.7	61.7	61.7
	Agree	15	25.0	25.0	86.7
	Neutral	1	1.7	1.7	88.3
	Disagree	3	5.0	5.0	93.3
	Strongly Disagree	4	6.7	6.7	100.0
	Total	60	100.0	100.0	

Table 4.17: Biometrics provides accountability

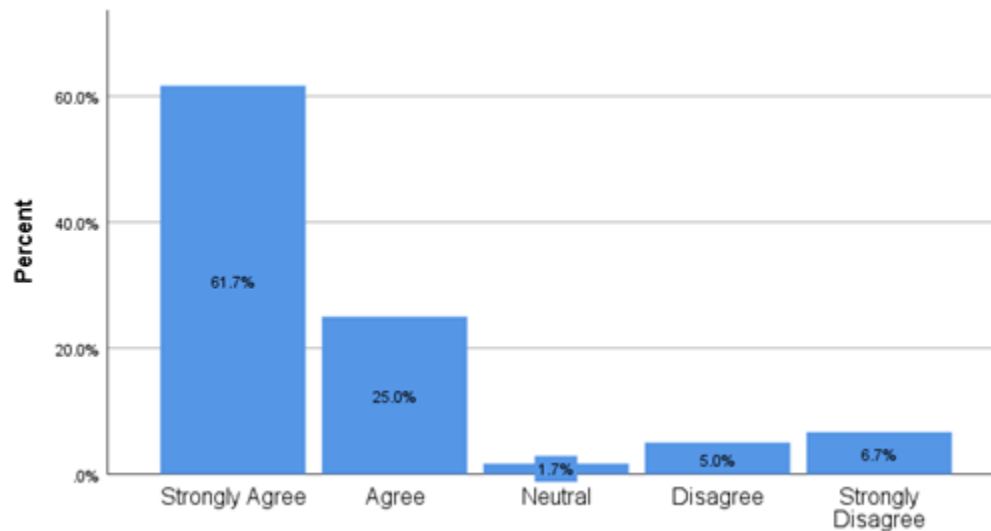


Figure 4.15: Biometrics provides accountability

The revealed Table 4.17 and Figure 4.15, stipulates that about 61.7% of respondents strongly agreed and 25.0% agreed that Biometrics provides accountability for individual usage. Less than 1.7% was neutral and possibly not sure. The study indicates that the number of respondents was 5.0% users disagreeing and just under 6.7% strongly disagree. This seriously assures that Biometrics does provide accountability for individuals as the most employees (86.7%) agreed.

According to Aithal (2015), Biometrics is a secure identification mechanisms allowing precise allocation of responsibility for fraud.

#### 4.6 SECTION D: Influencing Factors for use of Biometrics

Section D of the questionnaire was intended to determine the influencing factors of the KZN Provincial Treasury's decision to use biometric security. The frequencies are presented both numerically and in a percentage, format to reflect the respondents' responses which are further illustrated by using bar charts to facilitate data analysis.

The numerical values of 1= SA, 2=A, 3=N, 4=D, 5=SD which respectively represent strongly agree, agree, neutral, disagree and strongly disagree are used to illustrate the difference in responses of respondents. The tables 4.18 provides a numeric summary of the participants' responses with regards to the question asked in the questionnaire:

Questions	Total	Strongly Agree (%)	Agree (%)	Neutral (%)	Disagree (%)	Strongly Disagree (%)	Total (%)
Question 14	60	48%	33%	5%	12%	2%	100%
Question 15	60	30%	48%	8%	5%	8%	100%
Question 16	60	22%	38%	27%	12%	2%	100%
Question 17	60	38%	43%	7%	10%	2%	100%
Question 18	60	5%	28%	33%	30%	3%	100%

Table 4.18: Summary of question responses in section D

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	29	48.3	48.3	48.3
	Agree	20	33.3	33.3	81.7
	Neutral	3	5.0	5.0	86.7
	Disagree	7	11.7	11.7	98.3
	Strongly Disagree	1	1.7	1.7	100.0
	Total	60	100.0	100.0	

Table 4.19: Biometrics security adds value to service delivery

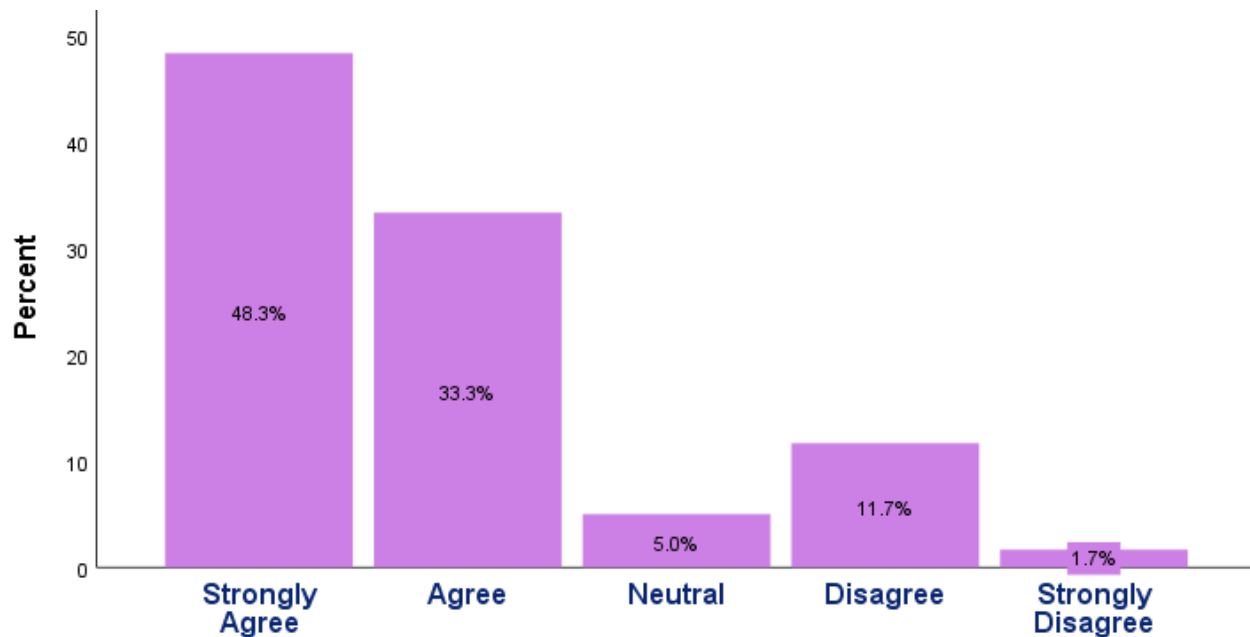


Figure 4.16: Biometrics security adds value to service delivery

Table 4.19 and Figure 4.16, about 48.3% of respondents strongly agreed and around 33.3% agreed that the implementation of Biometrics security has added value to service delivery. The 5.0% that was neutral therefore neither agreed nor disagreed that the implementation of Biometric security has added value to the service delivery or not. The study indicates that approximately 11.7% of respondents disagree and 1.7% strongly disagreed that the implementation of Biometrics security has added value to service delivery. This concludes that the implementation of Biometrics security has added value to service delivery as most employees (81.6%) have agreed. According to Giesing (2003), biometrics is accepted by individuals when it



adds value to service delivery that will include a security factor and increased accessibility through speed and ease of use.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	18	30.0	30.0	30.0
	Agree	29	48.3	48.3	78.3
	Neutral	5	8.3	8.3	86.7
	Disagree	3	5.0	5.0	91.7
	Strongly Disagree	5	8.3	8.3	100.0
	Total	60	100.0	100.0	

Table 4.20: Biometrics builds a good impression on employees

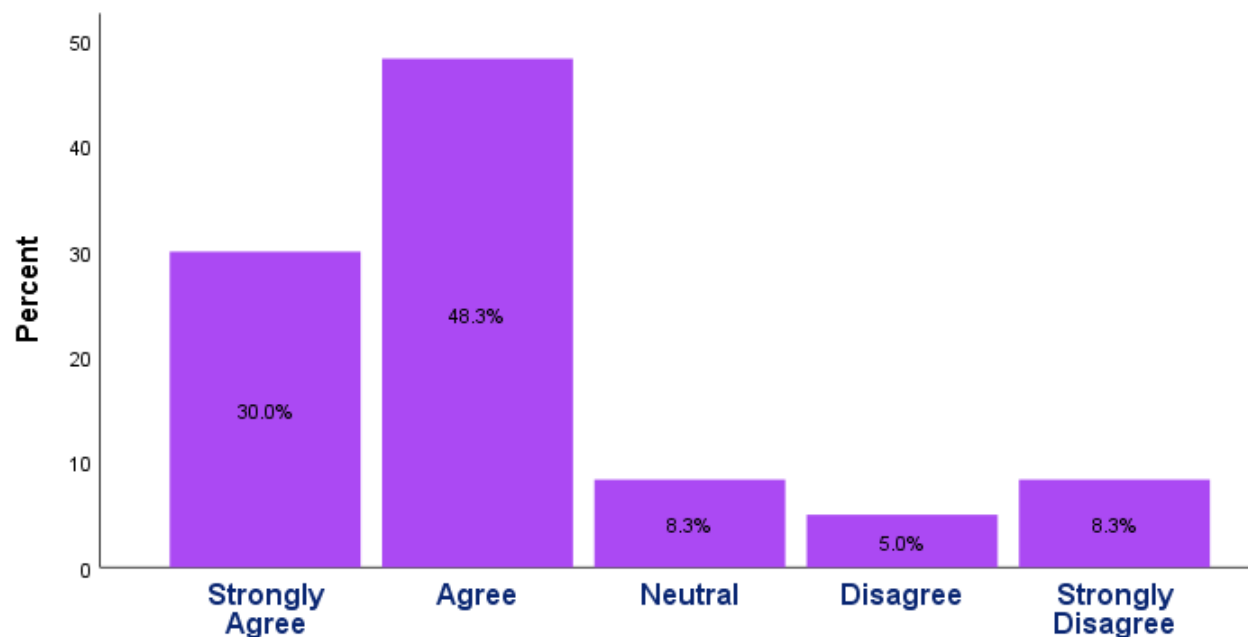


Figure 4.17: Biometrics builds a good impression on employees

As shown in Table 4.20 and Figure 4.17, 30.0% of respondents strongly agreed and 48.3% agreed that Biometrics built a good impression on the employees that are currently using Biometrics in IT security Management at KZN Treasury. 8.3% were neutral which specifies that the employees are not sure whether biometrics built a good impression towards them or not. The study indicates that the number of negative respondents was 5.0% users disagreeing and 8.3% strongly disagreeing that those biometrics built a good impression on the employees that are currently using Biometrics

in IT security Management at KZN Treasury. This confirms that the biometrics built a good impression on the employees that are currently using Biometrics in IT security Management at KZN Treasury as most employees (78.3%) have agreed. According to Giesing (2003), an individual can be identified within seconds with the Biometric identification systems and that will lead to improvement of customer service.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	13	21.7	21.7	21.7
	Agree	23	38.3	38.3	60.0
	Neutral	16	26.7	26.7	86.7
	Disagree	7	11.7	11.7	98.3
	Strongly Disagree	1	1.7	1.7	100.0
	Total	60	100.0	100.0	

Table 4.21: Re-enrolment and enrolment of multiple fingers mitigates errors

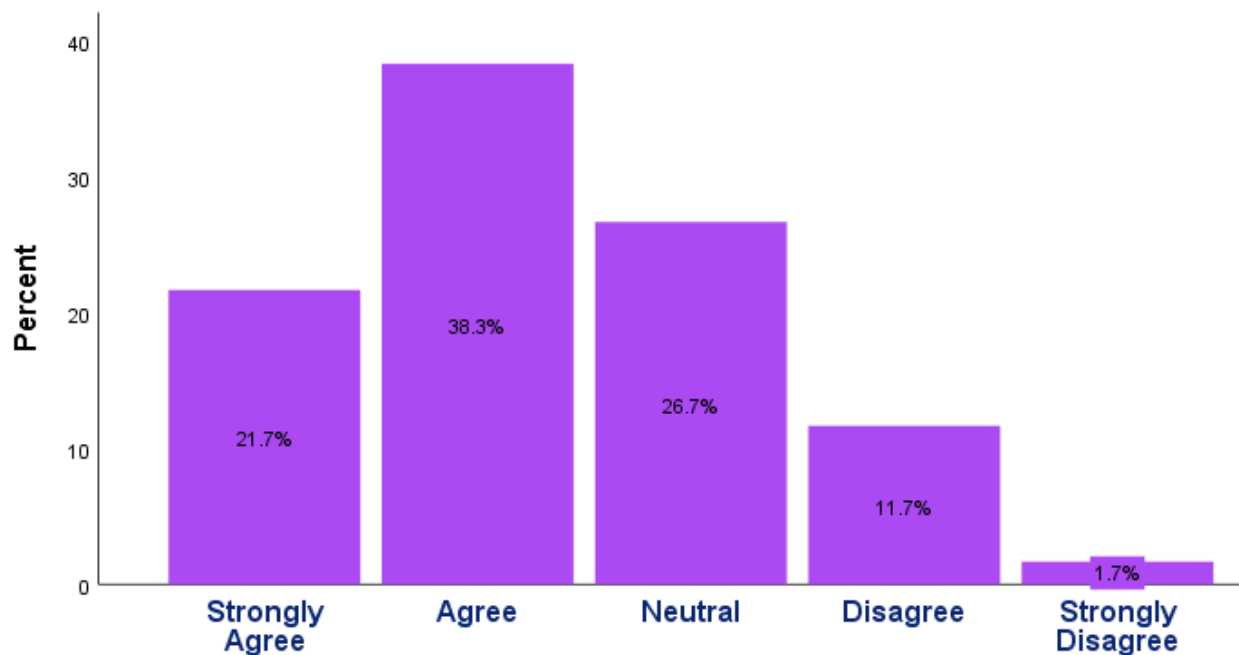


Figure 4.18: Re-enrolment and enrolment of multiple fingers mitigates errors

Table 4.21 and Figure 4.18 specified that 21.7% of respondents strongly agreed and around 38.3% agreed that re-enrolment and enrolment of multiple fingers mitigate errors.

Approximately 26.7% were neutral therefore specifying that a lot of employees neither agree nor

disagree or are unsure whether re-enrolment and enrolment of multiple fingers mitigate errors or not. Almost 11.7% of respondents disagreed and just under 1.7% strongly disagreed that that re-enrolment and enrolment of multiple fingers mitigate errors. This suggests that though 60% of employees agreed, employees are more divided on whether re-enrolment and enrolment of multiple fingers mitigate errors. The reason could be that most respondents are not Biometrics Enrolment Offices hence they would not know the technicalities of Biometrics which is why so many respondents were neutral.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	23	38.3	38.3	38.3
	Agree	26	43.3	43.3	81.7
	Neutral	4	6.7	6.7	88.3
	Disagree	6	10.0	10.0	98.3
	Strongly Disagree	1	1.7	1.7	100.0
	Total	60	100.0	100.0	

Table 4.22: Individuals being reliable in actions and activities

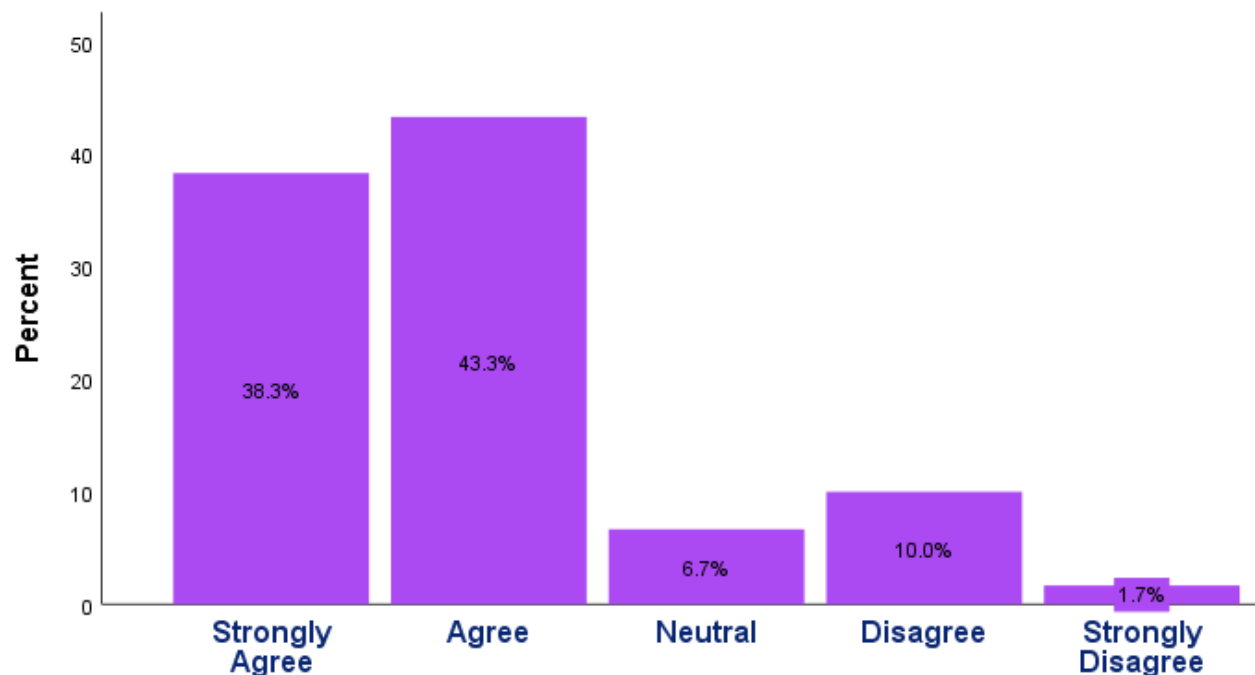


Figure 4.19: Individuals being responsible in actions and activities

Table 4.22 and Figure 4.19, stipulates that about 38.3% of respondents strongly agreed and around 43.3% agreed that the individuals are responsible in their actions and activities onto the financial systems BAS and Persal, as biometrics acts as the gateway to these systems. About 6.7% were neutral therefore this specifies that the employees are not sure or neither agree nor disagree with the statement. The study indicates that 10.0% of respondents disagree and 1.7% strongly disagreed that the individuals are reliable in their actions and activities onto the financial systems BAS and Persal, as biometrics acts as the gateway to these systems. This means that individuals can be relied on to be honest in their actions and activities onto the financial systems as most employees (81.6%) have agreed. According to Aithal (2015), Biometrics is a secure identification mechanism allowing precise allocation of responsibility for fraud.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	3	5.0	5.0	5.0
	Agree	17	28.3	28.3	33.3
	Neutral	20	33.3	33.3	66.7
	Disagree	18	30.0	30.0	96.7
	Strongly Disagree	2	3.3	3.3	100.0
	Total	60	100.0	100.0	

Table 4.23: Characteristics and challenges that makes difficult for decision making

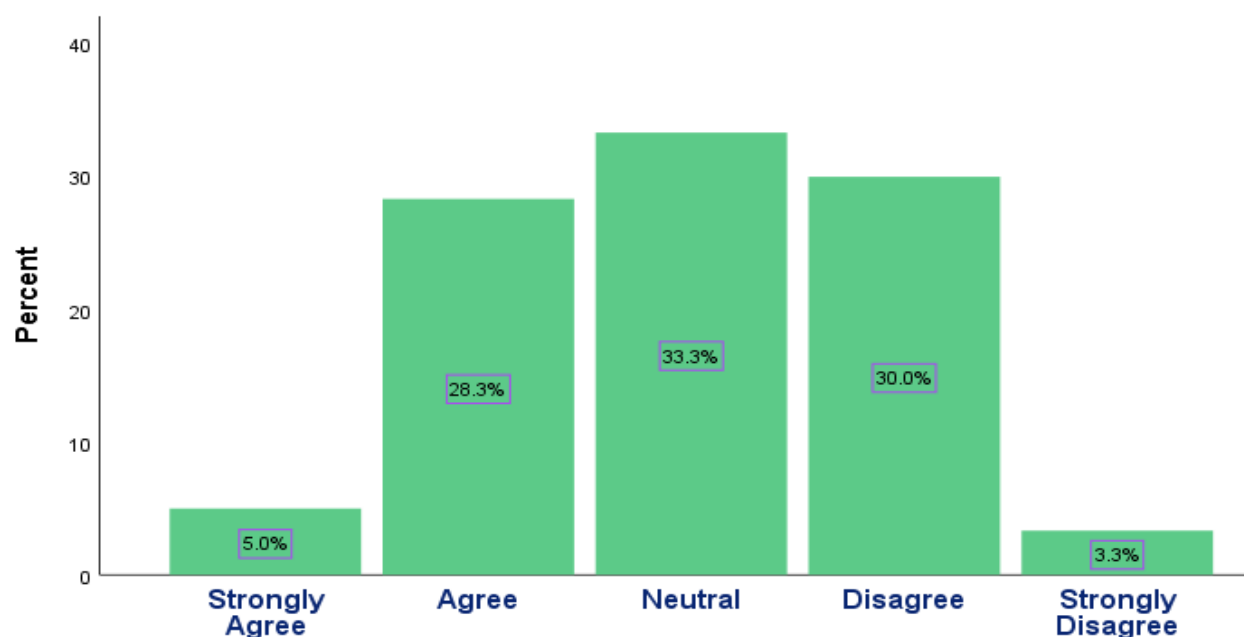


Figure 4.20: Characteristics and challenges that makes difficult for decisions making

Table 4.23 and Figure 4.20, stipulated that 5.0% of respondents strongly agreed and about 28.3% agreed that Biometrics has characteristics and challenges that make it difficult in making decisions. About 33.3% was neutral meaning that the employees neither agreed nor disagreed or are not sure whether Biometrics challenges makes difficult in making decisions or not. The study indicates that 30.0% of users disagree and around 3.3% strongly disagreed that Biometrics challenges make difficult in making decisions. This clarifies that there are differing opinions on whether Biometric security technology has characteristics and challenges that make it difficult in making decisions because 33% agree, 33% disagreed and 33% were neutral. It is possible that respondents did not understand the question.

#### **4.7 SECTION E: Technology Used**

Section E of the questionnaire was intended to determine the impact of government employees using biometrics in IT security management at the KZN treasury. It is also to establish if the KZN provincial treasury is using the most secure and latest technology in IT security management. The frequencies are presented both numerically and in a percentage format to reflect the respondents' responses which are further illustrated by using bar charts to facilitate data analysis.

The numerical values of 1= SA, 2=A, 3=N, 4=D, 5=SD which respectively represent strongly agree, agree, neutral, disagree and strongly disagree are used to illustrate the difference in the responses of respondents. Table 4.24 provides a numeric summary of the participants' responses with regards to the question asked in the questionnaire:

Questions	Total	Strongly Agree (%)	Agree (%)	Neutral (%)	Disagree (%)	Strongly Disagree (%)	Total (%)
Question 19	60	25%	42%	15%	13%	5%	100%
Question 20	60	15%	48%	22%	13%	2%	100%
Question 21	60	30%	45%	12%	8%	5%	100%
Question 22	60	30%	47%	7%	15%	2%	100%
Question 23	60	30%	47%	10%	8%	5%	100%

Table 4.24: Summary of question responses in section E

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	15	25.0	25.0	25.0
	Agree	25	41.7	41.7	66.7
	Neutral	9	15.0	15.0	81.7
	Disagree	8	13.3	13.3	95.0
	Strongly Disagree	3	5.0	5.0	100.0
	Total	60	100.0	100.0	

Table 4.25: Latest technology used for security control

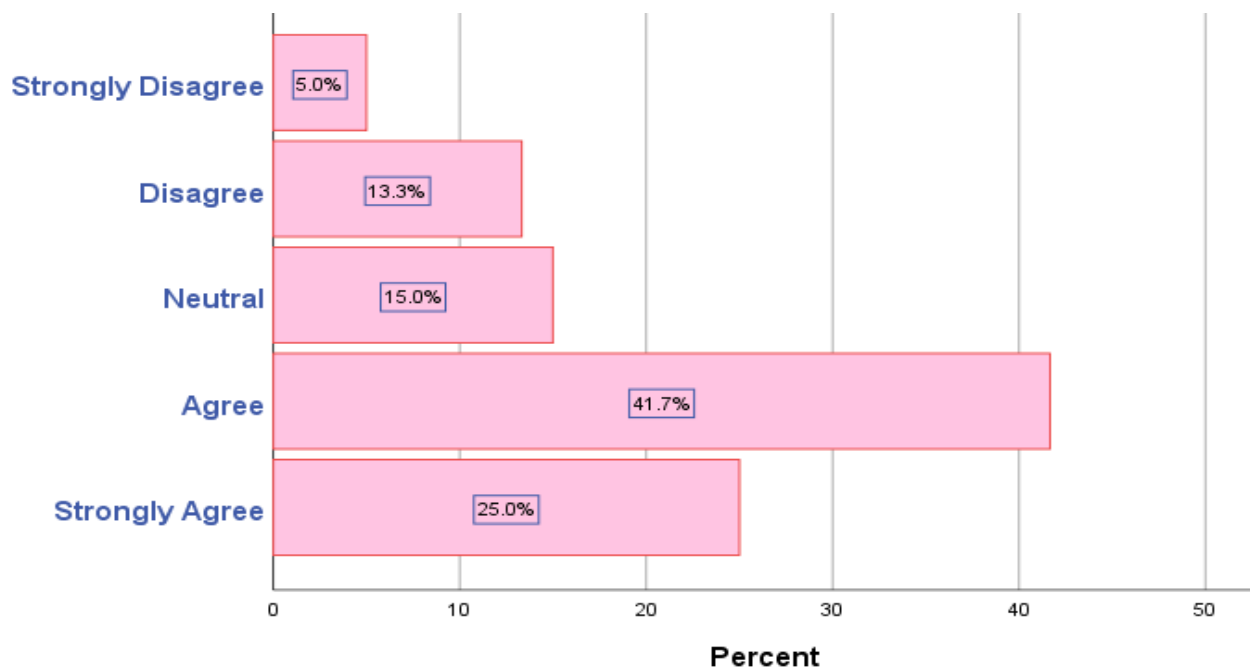


Figure 4.21: Latest technology used for security control

Table 4.25 and Figure 4.21, shows that 25.0% of respondents strongly agreed and about 41.7% agreed that Biometrics is the latest technology that is being used for security control. 15.0% was neutral therefore this stipulates that the employees are not sure whether Biometric is the latest technology or not. This study indicates that 13.3% of users disagree and 5.0% strongly disagree that Biometric is the latest technology that is being used for security control. This means that most respondents (66.7%) agree the Biometric is the latest technology that is being used for security control. These days, Biometrics-based authentication has become progressively appealing and common for most of the human-computer interaction devices, Buciu and Gacsadi (2016).

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	9	15.0	15.0	15.0
	Agree	29	48.3	48.3	63.3
	Neutral	13	21.7	21.7	85.0
	Disagree	8	13.3	13.3	98.3
	Strongly Disagree	1	1.7	1.7	100.0
	Total	60	100.0	100.0	

Table 4.26: KZN Treasury using the most secured and latest technology

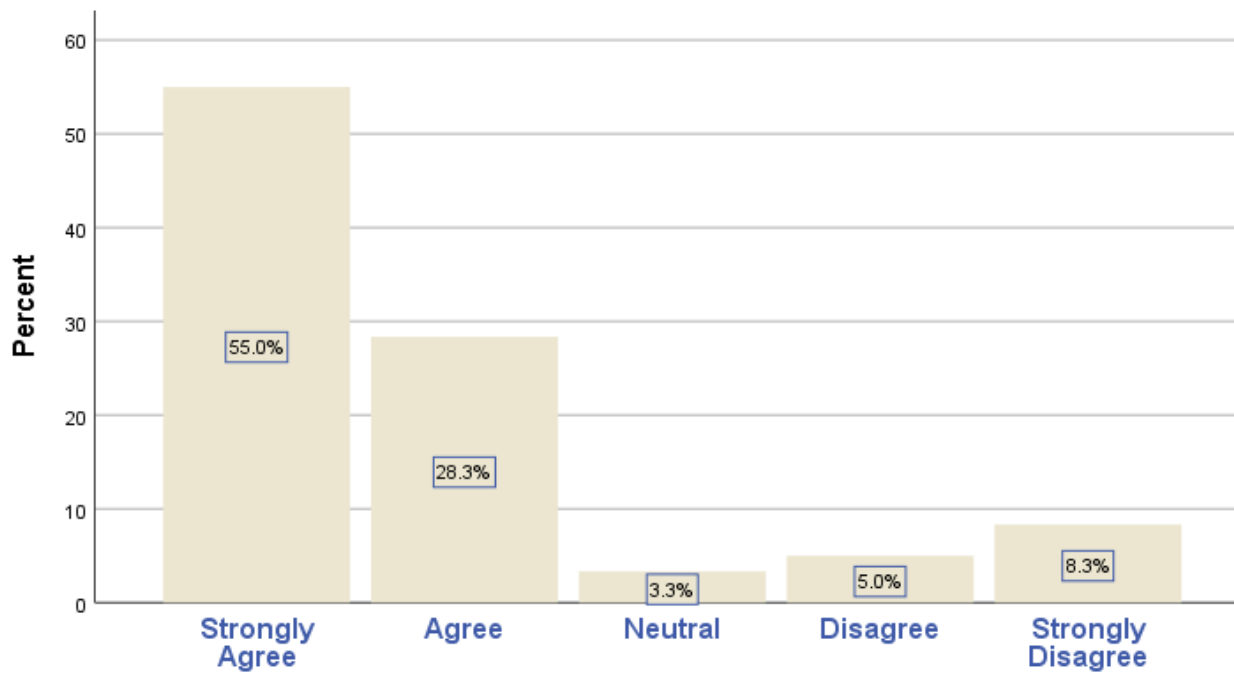


Figure 4.22: KZN Treasury using the most secured and latest technology

Table 4.26 and Figure 4.22, outlines that 55.0% respondents strongly agreed and 28.3% agreed that KZN Treasury is using the most secure and latest technology in managing security. 3.3% was neutral therefore this means that the respondents are not sure whether KZN Treasury is using the most secure and latest technology in managing security or not. 5.0% of respondents disagree and 8.3% strongly disagreed that KZN Treasury is using the most secure and latest technology in managing security. In summary, 83.3% of respondents agree that KZN Treasury is using the most secure and latest technology in managing security.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	18	30.0	30.0	30.0
	Agree	27	45.0	45.0	75.0
	Neutral	7	11.7	11.7	86.7
	Disagree	5	8.3	8.3	95.0
	Strongly Disagree	3	5.0	5.0	100.0
	Total	60	100.0	100.0	

Table 4.27: Biometrics fingerprint feature provides accurate security control



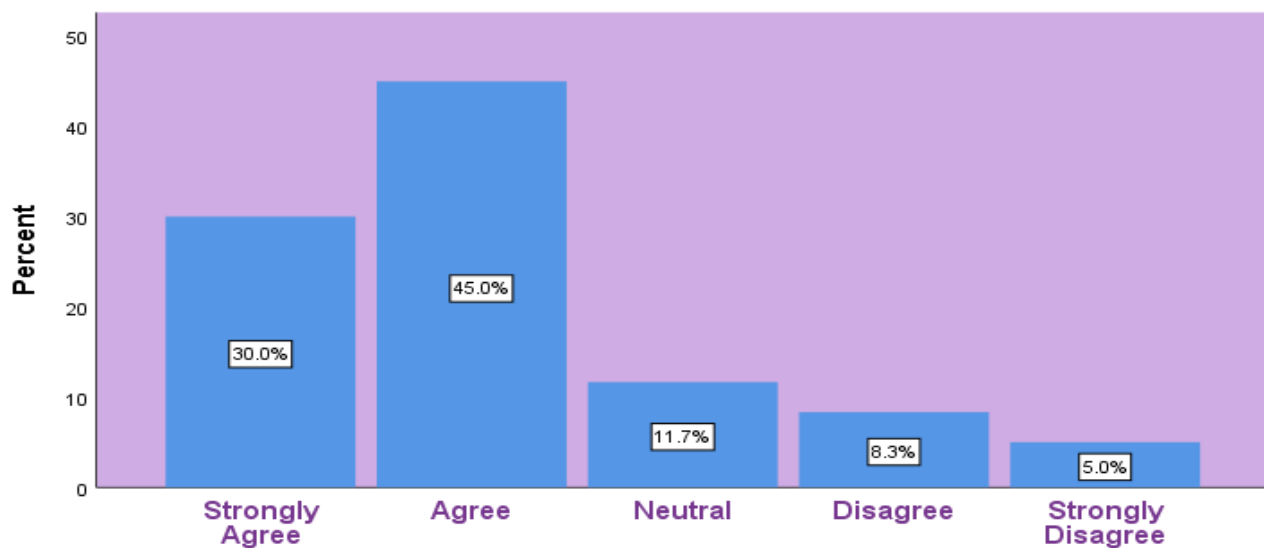


Figure 4.23: Biometrics fingerprint feature provides accurate security control

As shown in Table 4.27 and Figure 4.23, 30.0% of respondents strongly agreed and 45.0% agreed that the Biometrics fingerprint feature provides an accurate security control. Just under 11.7% was neutral therefore this means that the employees are not sure whether the Biometrics fingerprint feature provides an accurate security control or not. 8.3% of users disagreed and 5.0% strongly disagreed that Biometric fingerprint features provide accurate security control. We can conclude that Biometrics fingerprint features provide an accurate security control as most respondents (75%) have agreed. According to Bhagavatula et al. (2015), there are advantages that the users do not have to carry or remember anything such as pin or password. According to Faridah et al. (2016) urged that biological traits such as fingerprints are reliable in performance and are much better as compared with behavioural traits such as signature, voice or keystroke.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	18	30.0	30.0	30.0
	Agree	28	46.7	46.7	76.7
	Neutral	4	6.7	6.7	83.3
	Disagree	9	15.0	15.0	98.3
	Strongly Disagree	1	1.7	1.7	100.0
	Total	60	100.0	100.0	

Table 4.28: Technology used provides a secured and reliable user identity

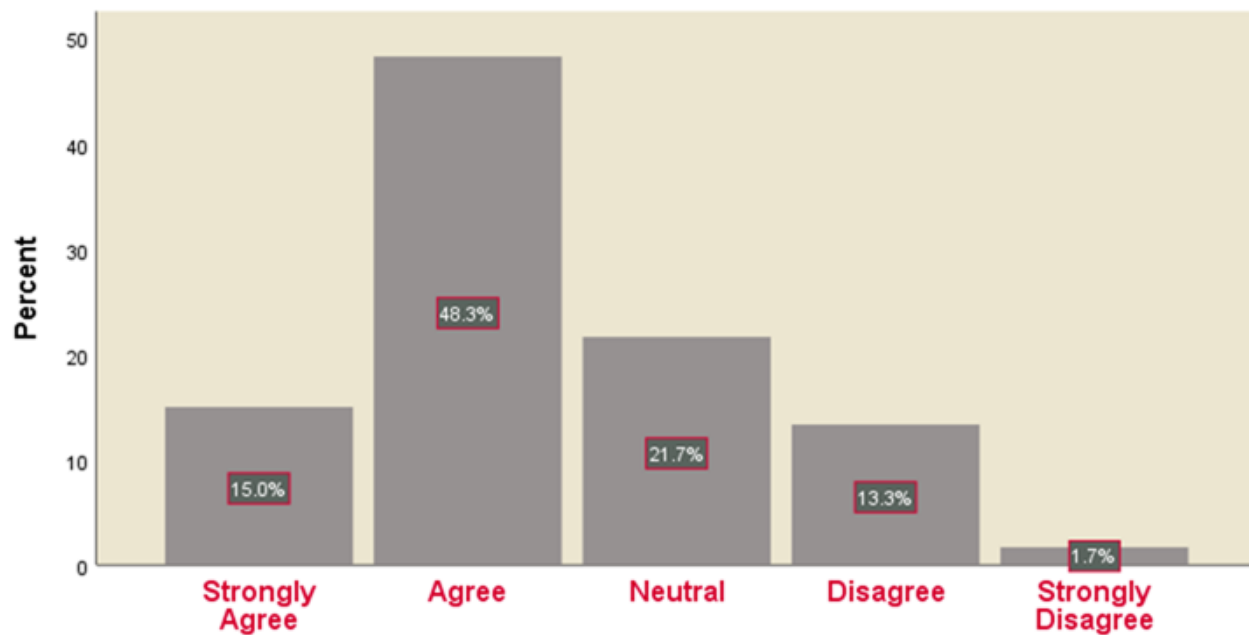


Figure 4.24: Technology used provides a secure and reliable user identity

As shown in Table 4.28 and Figure 4.24 above, 15.0% of respondents strongly agreed and about 48.3% agreed that the technology used provided a secure user identity and reliability. Almost 21.7% was neutral meaning that these respondents are not sure whether the technology used to provide a secure user identity and reliability or not. 13.3% of respondents disagreed and 1.7% strongly disagreed with the statement. We can conclude that the technology used is secure and reliable as most respondents (63.3%) have agreed. Faridah et al. (2016), referred to Biometrics as biometrics identification due to the fact that a person can be automatically recognised based on their physiological characteristics, therefore, every person has their own exclusive characteristics that explain their personal identity.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	18	30.0	30.0	30.0
	Agree	28	46.7	46.7	76.7
	Neutral	6	10.0	10.0	86.7
	Disagree	5	8.3	8.3	95.0
	Strongly Disagree	3	5.0	5.0	100.0
	Total	60	100.0	100.0	

Table 4.29: Using the latest technology makes users feel at ease

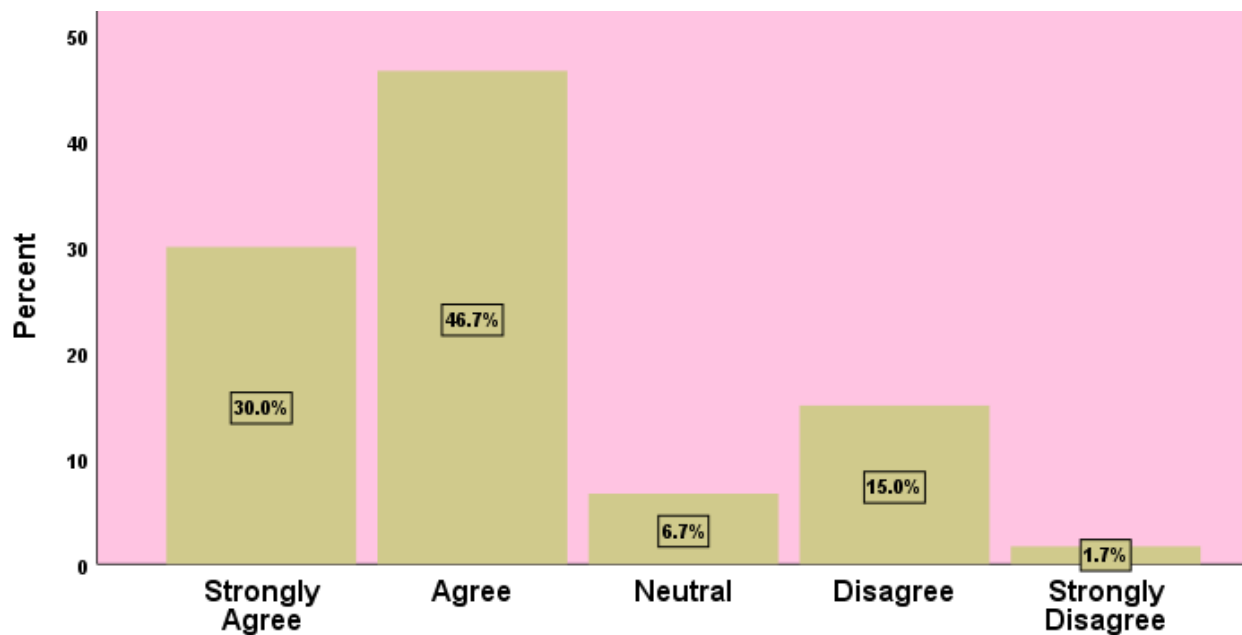


Figure 4.25: Using the latest technology makes users feel at ease

As shown in Table 4.29 and Figure 4.25, 30.0% of respondents strongly agreed and almost 46.7% agreed that using the latest technology makes users feel at ease. Just under 6.7% was neutral meaning that the respondents are not sure or neither agree or disagree with the statement. 15.0% of respondents disagreed and 1.7% strongly disagreed with the statement. In summary, using the latest technology makes users feel at ease as most employees (76.7%) have agreed. The security reasons for rolling out fingerprint authentication has been accumulating in several institutions for different purposes because of the ease of use method in comparison to the older methods which used physical inking of individual fingerprint that the users found it difficult to removing the ink later on (Alsaadi, 2015).

#### 4.4 Conclusion

In this Chapter, the findings were analysed in detail to be able to produce an accurate data analysis. The analysis has revealed that most respondents have agreed on most questions regarding the impact of Government Employees using Biometrics in IT Security Management at the KZN Treasury. This means that KZN Treasury IT employees see the introduction of Biometrics as a positive step in all aspects of security, monitoring, control, accountability, technology, user-friendliness, and management of systems, people and information. Very few

respondents were neutral (not sure or neither agreed nor disagreed) on whether Biometrics has contributed towards the department and what impact it has created on the government employees. There was a fairly constant number of respondents that disagreed or strongly disagreed with the majority view. The reasoning for this negative perception of Biometrics would need a qualitative analysis, but since the research was anonymous, we will never know why this small group disagreed with the majority view.

The analysis should facilitate the interpretation that will lead to meaningful conclusions and recommendations in chapter five so as to complete the study. The Department can take lessons from this research for future endeavours regarding the Biometrics system.

## **CHAPTER 5**

### **5.0 CONCLUSION AND RECOMMENDATIONS**

#### **5.1 Introduction**

The previous chapter presentation was on the data analysis and interpretation in relation to the negative and positive factors which contributed to the impact of employees using biometrics in IT security management. This chapter deals with the conclusions of the study which are the findings, recommendations, limitations and implications for further research studies. The chapter will also provide some applicable findings that could assist the Department of KZN Provincial Treasury in the future regarding Biometrics and new technology implementations and its impact on employees.

#### **5.2 Objectives of the Study**

The main objective of the study was to determine the influencing factors of KZN Provincial Treasury's decision to use biometric security.

The second objective of the study was to determine the impact of government employees using biometrics in IT Security Management at KZN Treasury.

The third objective of the study was to determine the impact of biometric security on work performance at KZN Provincial Treasury.

The last objective of the study was to determine whether the implementation of biometric security has added value to service delivery.

#### **5.3 Population of the Study**

The research population was obtained from the Biometrics database at KZN Treasury. The sampling of this study was the stratified sampling method. The researcher believed that the most reliable information collected from the research questions could be gained from this sample. The questionnaires were given to 70 participants but only 60 respondents were willing to participate. Therefore only 60 respondents took part in this research. The responses were coded for an easy analysis using SPSS and Excel programs and the analysis and interpreted presentation in chapter 4 by utilising the frequency and percentage tables and charts.

## 5.4 Cronbach's Alpha

Case Processing Summary			
		N	%
Cases	Valid	60	100.0
	Excluded <sup>a</sup>	0	.0
	Total	60	100.0

Table 5.1: Case processing summary

The table 5.1 interpretation is the total sample was 60 equating to 100% case participation with nil exclusions.

According to Cronbach's alpha, the reliability statistics are interpreted as below table.

Cronbach's alpha	Internal consistency
$0.9 \leq \alpha$	Excellent
$0.8 \leq \alpha < 0.9$	Good
$0.7 \leq \alpha < 0.8$	Acceptable
$0.6 \leq \alpha < 0.7$	Questionable
$0.5 \leq \alpha < 0.6$	Poor
$\alpha < 0.5$	Unacceptable

Table 5.2: Cronbach's alpha the reliability statistics

Reliability Statistics		
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.933	.933	20

Table 5.3: Reliability statistics

Cronbach's alpha measures the internal consistency reliability when using Likert-type scales. Therefore, in the above table 5.3, it is noted that Cronbach's alpha is .933 which is a great result. The goal and the higher the value of Cronbach's alpha indicates the excellent consistency of the items in the scale. This shows that the questions that were used are excellent and it means they are reliable in terms of Cronbach's alpha measurements.

<b>Summary Item Statistics</b>							
	Mean	Minimum	Maximum	Range	Maximum / Minimum	Variance	N of Items
Item Means	2.178	1.700	3.400	1.700	2.000	.185	20
Inter-Item Correlations	.410	-.343	.809	1.151	-2.361	.091	20

Table 5.4: Summary item statistics

The number of items on the measurement instruments is 20. The mean (average) scoring is 2.178 which the researcher considers as good, with the minimum score of 1.7 and a maximum score of 3.4.

## 5.5 Findings of the Study

### **Objective 1: Determine the impact of Biometric security on work performance at KZN Provincial Treasury.**

This objective referred to the findings from questions in section B. The analysis of this study has revealed that respondents have responded positively as most have agreed to this objective. Very few respondents were neutral or in disagreement when it comes to Biometrics improving the quality of the work and providing greater control over their work. Biometrics access control systems guarantee that acceptable access measures are implemented to protect the critical systems from loss of information and unauthorized access. Therefore, almost everyone agreed that using Biometrics provides greater control over his or her work. Using biometrics will assist in improving the quality of work and better the service delivery in organisations and minimize fraud (Evans et al., 2015)

Biometrics ensures that adequate non-repudiation measures are implemented and leaves an audit trail database of critical transactions that are kept in a secured and protected data storage.

Therefore Biometrics enables system security control for users when accessing the financial systems, BAS and Persal.

The organisational impact of Biometrics is great because it provides a gateway to BAS and Persal systems for the Province of KZN, and its accessibility is important as many users will be unable to conduct their day-to-day duties should the system becomes unavailable. Furthermore, respondents agree that the Biometrics provides accurate information because it controls the entrance to the critical systems and provides non-repudiation services to the users accessing these critical systems from within the Province of KwaZulu-Natal. Biometrics will keep records of activities done by users as evidence if it is ever needed. Villaroman et al. (2018), states that Biometrics promotes transparency to the organization to save time in preparation of employee records as the system keeps on updating in real time.

**Objective 2: Determine whether the implementation of Biometric security has added value to service delivery.**

This objective referred to the findings from questions in section C. The analysis of this study revealed that most respondents agree that Biometrics has added value to service delivery. According to Giesing (2003), biometrics is accepted by individuals when it adds value to service delivery that will include a security factor and increased accessibility through speed and ease of use. The biometrics fingerprint system is popular as a security management measure and adds value to service delivery because it gives assurance and trustworthiness when gaining access to the system by operating in accordance with the PKI practices. Therefore, respondents have indicated on the analysis that they prefer using Biometrics fingerprint as security management measure than using other Biometric features like iris, voice and so on. Users feel that the biometric fingerprints system adds value to their service delivery because it provided assurance, accuracy and accountability to the user. Using the fingerprint method to access the system creates confidence, and is easy to use for the users (Hortai, 2018).

This study showed that perceptions of biometrics, the effectiveness of security, the necessity for this technology and reliability are more important considerations in a decision to recommend or adopt the technology. Biometrics was found not to be too complex though many respondents were neutral.



Respondents feel that it is easy to use Biometrics hence there is no training required for users and it prevents fraud. Biometrics is an identification technique that depends on the verification or recognition of a person based on distinctive physiological features. Respondents were divided on whether Biometrics is a monitoring and tracking system or a security system. Many respondents were neutral here too. None of the respondents are wrong or right because Biometrics performs security functions as well as monitoring and tracking functions. Accountability is part monitoring and control and part security, and nearly all respondents agreed that Biometrics provides accountability through the database audit trail of users' actions in logging into the financial systems.

In summary, it is clear that users of the Biometric security system are very satisfied with the use of the system at the KZN Treasury. Users do not feel overwhelmed by the tasks, choices, and work that security decisions require of them. They understand and comfortable that this system is actually making them more secure.

**Objective 3: Determine the influencing factors of KZN Provincial Treasury's decision to use Biometric security.**

This objective referred to the findings from questions in section D. The findings in this study revealed that most respondents have agreed that the main factor of the KZN Provincial Treasury's decision to use Biometrics security was to add value to service delivery within the Department. Furthermore, most respondents agreed that Biometrics builds a good impression on employees that are using Biometrics in IT Security Management at KZN Treasury. Provincial Treasury plays a very important role in the implementation and providing support of information systems both internally and externally within KZN Province's Government Departments. According to Hortai (2018), using Biometrics in IT Security Management is very important as it provides the purpose for granting access in line with the access rights of the authorised users, disallow unauthorized entities from accessing the system and builds a good impression on employees. The study reveals that respondents were equally split between agreeing, neutral and disagreeing that Biometrics has abilities and challenges that make it difficult in making decisions. The reason for the equal split of responses could be that this question was not clearly understood by respondents because the Biometric system does not have abilities and challenges that make it difficult in making decisions.

Regarding being responsible for their actions and activities when you log onto the system, respondents agreed that they are responsible for any actions they take on the system. It is secure, reliable and sufficiently protected by effective controls in order to provide secure and uninterrupted services delivery and trace any activities on the system down to the user. This reduces the major problem in of fraud in KZN Provincial Departments because Biometrics access control is put into operation to enhance access control in order to minimize fraud and provide related evidence pertaining to the BAS and Persal systems. Therefore, it is easy for management to trace transactions and take appropriate action. According to Aithal (2015), Biometrics is a secure identification mechanism allowing precise allocation of responsibility for fraud. The findings also revealed that the re-enrolment and enrolment of multiple fingers mitigate errors making it impossible for unauthorised users to access the system. There were many neutral responses to this question because users did not apply their minds to the benefits of enrolling with multiple fingers.

**Objective 4: Determine the impact of government Employees using Biometrics in IT Security Management at KZN Treasury.**

This objective referred to the findings from questions in section E. The findings revealed that most respondents agree that using the latest technology has a positive impact on government employees using biometrics in security control at KZN Treasury. KZN Treasury is using Biometric technology that is also used and trusted in financial institutions such as banks throughout South Africa. According to Lewandowski (2017), the most attractive solution in mobile banking and also solutions applied in branches of the banks is biometrics.

Though there were a number of respondents who were neutral, most agreed that the system implemented at KZN Treasury is new and secure technology for identification verification, increased convenience and security. Biometrics provides strong authentication technology in any application. Therefore, KZN Treasury is using the most secure and latest technology in managing security.

The respondents have also agreed that biometrics features such as fingerprint recognition can significantly increase security compared to the old passwords when it comes to accurate security control. Furthermore, the responses showed that using the latest technology makes the user feel at ease as the system authentication is fast and user-friendly, and only minimal user knowledge

and effort is required for the end user. Most of those surveyed showed very positive acceptability ratings for biometrics fingerprint scanners since it provides secure user identity and is reliable. Fingerprints cannot be easily stolen. According to Haas (2004), biometrics characteristics function as a persons' passwords to grant access to the system, they provide uniqueness to the person, can never be forged, or stolen

## **5.6 Recommendations**

Biometrics has been able to curtail fraud and corruption at KZN Treasury and in the provincial Government Departments. The employees must continue using Biometrics within KZN Treasury and Government Departments. This will ensure that the quality and control of work is not compromised. By doing this, work performance will continue to improve. Because Biometrics is the gateway to BAS and Persal, system availability is also crucial because the system holds critical information without which, work will stop.

Biometrics must be used for both security control, for monitoring and tracking because it has proved effective in both areas. Haas (2004), states biometrics uses the distinctive characteristics of an individual to be able to identify that person. KZN Treasury needs to ensure that they keep up with the latest international best practice in Biometrics. This they can see from other countries and from the banking industry. The use of fingerprints is ideal at the moment, but in the future, other technology methods like iris may be more effective. If the system was ever hacked or compromised, KZN would lose credibility.

Biometrics must always be user-friendly and any future changes and upgrades must be easy for users to use and for Government departments to implement. Using the fingerprint method to access the system creates confidence and is easy to use for the users (Hortai, 2018). Traceability is one of the advantages of biometrics so as to ensure that users are accountable for their transactions. Biometrics allows users to securely authorize transactions (Aithal, 2015). KZN Treasury needs to continue to add value to management and users as part of their mandate. The systems must be reliable and assist in decision-making. Whether using one or multiple fingers, Biometrics must be available and accurate at all times. Back-up and storage are crucial so that if fraud, corruption or performance issues are uncovered in the future, investigators can go back to the Biometrics system to get accurate user information and evidence.

Lastly, the technology used must always take into account the security, the monitoring and control functions of Biometrics. Technology is constantly improving and updating in the 4<sup>th</sup> industrial revolution so KZN Treasury must never be left behind. This means that KZN Treasury must use global benchmarks and understand what is happening globally with regards to Biometrics. This must be done while ensuring that systems and costs are user-friendly and manageable.

## **5.7 Limitations and Implications for further research**

The study found some limitations that may result in it not being perfect. There were several problems and challenges that the researcher encountered while conducting the research for this dissertation.

The challenge was to recruit an adequate number of participants. The formation of the initial database for some users took a long time, and many times the requests of the researcher were turned down because most of the users were extremely busy with their day-to-day functions to allow the opportunity for the research. Thus access to the participants and obtaining permission for the research was a major challenge.

Another challenge was that, the researcher was restricted in terms of the time to engage with the users, enrolment offers and management. This resulted in the choice of using a more proficient method, the questionnaire, rather than the more time-consuming methods such as the focus groups or participant observation.

Thirdly, the respondents knew the researcher. There is a possibility that some of them might have been subjective in their responses to the questionnaire.

Fourthly, there was a problem with data collection. Some of the respondents were unwilling to participate in the study saying that they do not use biometrics though they were registered as users of Biometrics for the financial systems.

There are numerous implications for future research in this study. Similar studies can be conducted in other government departments where employees are using biometrics. A similar study can be conducted using a larger or wider number of participants; this could improve on the results and make it easier to generalize. More detailed data analysis strategies can be conducted in the study. The responses from this study could be unpacked further with focus groups and interviews so as to get more specific information. This study only touches on four areas of Biometrics, which are Perceived Usefulness, Perceived Ease of Use (user satisfaction and organizational impact), Influencing Factors, and Technology and Security. This study is not aimed to cover a full and detailed list of biometric techniques.

Future study effort could focus on the relative impact of technical issues versus perceptions and attitudes of employees. Such a study reveals surprising results regarding technical issues rather than the impact of employees in using Biometrics. Lastly, a mixed method approach that combines quantitative and qualitative methods can be utilised in order to obtain more comprehensive responses. Depending on the research objectives, this study can be used as the basis of many more Biometric studies with specific topics like Security Control or Monitoring and Tracking or Technology Options or Organisational Impact.

## **5.8 Conclusion**

According to KZN Treasury and the researcher's findings, the biometric security system is successful in managing access to critical systems and allowing non-repudiation services. All users have to access BAS and Persal systems within the Province of KwaZulu-Natal using Biometrics as an authentication method of an individual's claimed identity. It is secure, reliable and easy to use. Using the fingerprint method to access the system creates confidence and is easy to use for the users (Hortai, 2018).

According to the findings, the researcher concluded that the use of the Biometrics security system has created a good impact on the work performance of the employees of KZN Treasury. It appears that the majority of the respondents believe that it has had a significant and positive effect on the level of work performance. This paper only touches on four areas of Biometrics, which are Perceived Usefulness, Perceived Ease of Use (user satisfaction and organizational impact), Influencing Factors and Technology and Security. These areas can still be studied

further, but the result of this study is clear: According to the findings, the decision to use Biometrics at KZN Treasury and for KZN Government Departments using BAS and Persal systems has been a good one and most people agree. The agreement is very high amongst KZN Treasury Management, users and Enrolment Officers on the positive effects of Biometrics in the Province.

Intensive work is still on-going to improve performance and attitudes towards Biometrics. The research also noticed that the one way to strengthen authentication mechanism is by using multiple factors of authentication. Technology in Biometrics is evolving every day and it is important that KZN Treasury keeps abreast with this so that security and traceability are never compromised.

Considering the questions and responses, the researcher can conclude that the perceptions and attitudes of biometrics users are positive. The users also trust that the Biometric security system is user-friendly and makes their duties much easier, better and quicker to conduct.

## 5.9 References

- Aithal, P. 2015. Biometric Authenticated Security Solution to Online Financial Transactions.
- Alsaadi, I. M. 2015. Physiological Biometric Authentication Systems, Advantages, Disadvantages And Future Development: A Review. *International Journal of Scientific & Technology Research*, 4, 285-289.
- Ananth, S. Biometrics and Its Impact in India. *We are happy to present the next edition of our Staff Paper Series. The series has been helping the Institute in presenting the academic work carried out by our faculty in various areas related to banking technology. The theme of the current edition is Biometrics. The world in general, and banking sector in particular, has been working on*, 119.
- Berini, D. J., van Beek, G. A., Arnon, I., Shimek, B. J., Fevens, R. B. & Bell, R. L. 2016. Enrollment kiosk including biometric enrollment and verification, face recognition and fingerprint matching systems. Google Patents.
- Bhagavatula, R., Ur, B., Iacovino, K., Kywe, S. M., Cranor, L. F. & Savvides, M. 2015. Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption.
- Blanche, M. T., Blanche, M. J. T., Durrheim, K. & Painter, D. 2006. *Research in practice: Applied methods for the social sciences*, Juta and Company Ltd.
- Bryman, A. & Bell, E. 2015. *Business research methods*, Oxford University Press, USA.
- Buciu, I. & Gacsadi, A. 2016. Biometrics systems and technologies: a survey. *International Journal of Computers Communications & Control*, 11, 315-330.
- Carroll, T. 2016. *Employee Perceptions of Biometric Security Adoption in the Workplace*, Northcentral University.
- De Luca, A., Hang, A., von Zezschwitz, E. & Hussmann, H. I feel like I'm taking selfies all day!: towards understanding biometric authentication on smartphones. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2015. ACM, 1411-1414.
- De Luca, S. N., ZIKO, I., SOMINSKY, L., NGUYEN, J. C., DINAN, T., MILLER, A. A., JENKINS, T. A. & SPENCER, S. J. 2016. Early life overfeeding impairs spatial memory performance by reducing microglial sensitivity to learning. *Journal of neuroinflammation*, 13, 112.
- Delone, W. H. & McLean, E. R. 2004. Measuring e-commerce success: Applying the DeLone & McLean information systems success model. *International Journal of electronic commerce*, 9, 31-47.
- Dunn, W. B., Broadhurst, D. I., Atherton, H. J., Goodacre, R. & Griffin, J. L. 2011. Systems level studies of mammalian metabolomes: the roles of mass spectrometry and nuclear magnetic resonance spectroscopy. *Chemical Society Reviews*, 40, 387-426.
- Evans, N., Marcel, S., Ross, A. & Teoh, A. B. J. 2015. Biometrics security and privacy protection [from the guest editors]. *IEEE Signal Processing Magazine*, 32, 17-18.
- Faridah, Y., Nasir, H., Kushsairy, A., Safie, S. I., Khan, S. & Gunawan, T. S. 2016. Fingerprint Biometric Systems. *Trends in Bioinformatics*, 9, 52-58.
- Felkins, J. F. 2015. Biometric data-driven application of vehicle operation settings. Google Patents.
- Giesing, I. 2003. *User perceptions related to identification through biometrics within electronic business*. University of Pretoria.
- Haas, E. P. 2004. Back to the Future-The Use of Biometrics, Its Impact of Airport Security, and How This Technology Should Be Governed. *J. Air L. & Com.*, 69, 459.
- Harinda, E. & Ntagwirumugara, E. 2015. Security & privacy implications in the placement of biometric-based ID card for Rwanda Universities. *Journal of Information Security*, 6, 93.

- Hortai, F. 2018. Possibilities of dynamic biometrics for authentication and the circumstances for using dynamic biometric signature. *Journal of Systems Integration*, 9, 3-18.
- Koteswari, S., Paul, P. J., Dheeraj, A. & Kone, R. 2016. Fusion of Iris and Fingerprint Biometric Identifier for ATM Services: An Investigative Study. *International Journal of Communications, Network and System Sciences*, 9, 506.
- Kukula, E. P. & Proctor, R. W. Human-biometric sensor interaction: Impact of training on biometric system and user performance. Symposium on Human Interface, 2009. Springer, 168-177.
- Kumar, R. 2019. *Research methodology: A step-by-step guide for beginners*, Sage Publications Limited.
- Kwakye, M. M., Boforo, H. Y. & Badzongoly, E. L. Adoption of Biometric Fingerprint Identification as an Accessible, Secured form of ATM Transaction Authentication. IJACSA.
- Layton, T. P. 2016. *Information Security: Design, implementation, measurement, and compliance*, Auerbach Publications.
- Lewandowski, R. 2017. Biometrics—new applications. *Przegląd Bezpieczeństwa Wewnętrznego*, 9, 381-392.
- Morosan, C. 2016. Opportunities and challenges for biometric systems in travel: A review.
- Narang, S., Kaur, S. & Mahajan, S. Biometric Attendance System.
- Nelson, W. B., Nelson, R. S. & Nickle, G. A. 2015. Infection control monitoring system. Google Patents.
- Oko, S. & Oruh, J. 2012. Enhanced ATM security system using biometrics. *International Journal of Computer Science Issues (IJCSI)*, 9, 352.
- Oye, N. & Nathaniel, J. 2018. Fraud Detection and Control System in Bank Using Finger Print Simulation.
- Pagnin, E. & Mitrokotsa, A. 2017. Privacy-preserving biometric authentication: challenges and directions. *Security and Communication Networks*, 2017.
- Pradhan, M. 2015. Next Generation Secure Computing: Biometric in Secure E-transaction. *International Journal*, 3.
- Prasanna, G. A., Anandakumar, K. & Bharathi, A. 2016. Multi Modal Biometric Systems: A State of the Art Survey.
- Rahman, M. 2016. *The Advantages and Disadvantages of Using Qualitative and Quantitative Approaches and Methods in Language "Testing and Assessment" Research: A Literature Review*.
- Rahman, M. M., Karmaker, A., Hasan, M. M. & Ahmed, S. 2015. Ensuring Quality in Biometric Systems. *International Journal of Security and Its Applications*, 9, 153-160.
- Rotich, E. K., Ikoha, A. P. & Wasike M, J. 2017. Biometric Properties for Identification in a Secure E-voting Application.
- Saunders, M. N. & Rojon, C. 2014. There's no madness in my method: explaining how your coaching research findings are built on firm foundations. *Coaching: An International Journal of Theory, Research and Practice*, 7, 74-83.
- Thirumoorthi, C. 2018. Fingerprint Based Authentication Using Image Processing Techniques.
- Tock, E. 2015. *The impact of employee activity monitoring in the employee and employer relationship & implications for privacy*. Utica College.
- van Maanen, J. 2016. *Biometrics and Intelligence: A Match Made in Heaven?*, Nederlandse Defensie Academie.
- Villaroman, G. A. C., San Pedro, A. B., Bacani, K. M., Clerigo, E. R. & Hipos, A. T. 2018. The Use of Biometric Attendance Recording System (BARS) and Its Impact on the Work



Performance of Cabanatuan City Government Employees. *Open Access Library Journal*, 5, 1.

Zhang, Z. H., JhaverI, D. J., Marshall, V. M., Bauer, D. C., Edson, J., Narayanan, R. K., Robinson, G. J., Lundberg, A. E., Bartlett, P. F. & Wray, N. R. 2014. A comparative study of techniques for differential expression analysis on RNA-Seq data. *PloS one*, 9, e103207.

## APPENDIX

### Appendix 1: Gatekeeper Letter

Private Bag X54001 Durban 4000  
South Africa  
www.UKZN.ac.za



**The Head of Department**  
**145 Chief Albert Luthuli Road**  
**Pietermaritzburg 3201**  
**Private Bag X9082**  
**Pietermaritzburg 3200**  
**Tel: 033 897 4200 – Fax 033 342 4662**

**SUBJECT: REQUEST FOR PERMISSION TO CONDUCT RESEARCH WITH KZN  
PROVINCIAL TREASURY OFFICIALS**

Dear Mr Magagula

I am currently pursuing a Master's in Information Systems and Technology through UKZN with bursary funding from Treasury. I kindly request permission to conduct research (questionnaire/survey based). A sample of 50 participants are targeted and they would be required to complete a questionnaire of 18 questions. The average time taken to complete would be 15 – 30 minutes which can be completed in their own time.

#### **Research Details and Motivation for Research**

##### **Research Topic –**

The Impact of Government Employees Using Biometrics in IT Security Management at KZN Treasury.

##### **Motivation**

The context of this research is Biometrics as an IT Security Management system and the impact of employees using it.

The anonymity/ confidentiality will be protected by ensuring that the names and other related personal information of the participants will not be required. The names of the participants is not required.

This study will contribute towards the body of knowledge since it will make people understand and resolve problems concerning the Biometrics security system. There is a need to conduct this study to be able to assess and measure the perspectives and the impact on employees towards using the Biometrics Security technology.

There is an accumulative need for improved controlled security and the growing capacities of electronic transactions are presently conducted transversely wired and wireless networks and technology is changing constantly. This has formed a strong necessity for additional consistent identity management. The identity management system verifies that identifying an individual as a crucial undertaking.

The objective of this study will determine: -

- The influencing factors of KZN Provincial Treasury's decision to use biometric security.
- The impact of government Employees using biometrics in IT Security Management at KZN Treasury.
- The impact of biometric security on work performance at KZN Provincial Treasury.
- Whether the implementation of biometric security has added value to service delivery.

For any further information kindly contact 083 7492177 or the supervisor on 033 260 7013,  
email Trishana Ramluckan <RamluckanT@ukzn.ac.za>

Thank you for your time and consideration this matter

Yours sincerely

  
.....  
**Mrs N Ndaba**  
**IT Governance Specialist**

Date 05.12.2018

**KWAZULU-NATAL**  
**PROVINCIAL TREASURY**  
**HEAD OF DEPARTMENT**  
  
2019 -02- 04  
P.O. BOX 3613, PIETERMARITZBURG

I hereby grant the candidate to conduct research using Biometrics as an IT Security Management system at KZN Provincial Treasury

  
.....  
**Mr LS Magagula**  
**Head of Department – KZN Provincial Treasury**

05/12/2018  
Date

## Appendix 2: Ethical Clearance Letter



11 February 2019

Mrs Nomkhosi Ndaba 217079556  
School of Management, IT and Governance  
Westville Campus

Dear Mrs Ndaba

Protocol reference number: HSS/2074/018M

Project title: The impact of Government employees using Biometrics in IT Security Management at KZN Treasury

### Full Approval – Expedited Application

In response to your application received 9 November 2018, the Humanities & Social Sciences Research Ethics Committee has considered the abovementioned application and the protocol has been granted **FULL APPROVAL**.

Any alteration/s to the approved research protocol i.e. Questionnaire/Interview Schedule, Informed Consent Form, Title of the Project, Location of the Study, Research Approach and Methods must be reviewed and approved through the amendment /modification prior to its implementation. In case you have further queries, please quote the above reference number.

PLEASE NOTE: Research data should be securely stored in the discipline/department for a period of 5 years.

The ethical clearance certificate is only valid for a period of 3 years from the date of issue. Thereafter Recertification must be applied for on an annual basis.

I take this opportunity of wishing you everything of the best with your study.

Yours faithfully

Dr Shamila Naidoo (Deputy Chair)  
Humanities & Social Sciences Research Ethics Committee

/pm

cc Supervisor: Dr Trishana Ramluckan  
cc Academic Leader Research: Professor Isabel Martins  
cc School Administrator: Ms Angela Pearce

---

Humanities & Social Sciences Research Ethics Committee

Dr Rosemary Sibanda (Chair)

Westville Campus, Govan Mbeki Building

Postal Address: Private Bag 354001, Durban 4000

Telephone: +27 (0) 31 200 3587/3550/4557 Facsimile: +27 (0) 31 200 4600 Email: [sibanda@ukzn.ac.za](mailto:sibanda@ukzn.ac.za) / [ishtar@ukzn.ac.za](mailto:ishtar@ukzn.ac.za) / [melvyn@ukzn.ac.za](mailto:melvyn@ukzn.ac.za)

Website: [www.ukzn.ac.za](http://www.ukzn.ac.za)

## Appendix 3: Informed Consent Form

### UKZN HUMANITIES AND SOCIAL SCIENCES RESEARCH ETHICS COMMITTEE (HSSREC)

#### APPLICATION FOR ETHICS APPROVAL For research with human participants

##### Information Sheet and Consent to Participate in Research

Date: 28 November 2018

Greetings,

My name is Nomkhosi Ndaba from the School of Management, IT and Governance, my contact number is 083 749 2177 and my email address is [nomkhosin106@gmail.com](mailto:nomkhosin106@gmail.com).

You are being invited to consider participating in a study that involves research an analysis of the impact of Government Employees Using Biometrics in IT Security Management at KZN Treasury. The aim and purpose of this research is to unpack aspects that are leading to the influencing factors of KZN Provincial Treasury's decision to use biometric security and the influence that the use of Biometric Security have on work performance at KZN Treasury. The study is expected to include 50 participants in total drawn from KZN Provincial Treasury's, 13 questions will be given to the participants. It will involve the following procedures, the researcher will hand deliver the questionnaires to the individuals who are willing to participate on this research. The researcher will introduce herself and try to respond to all queries that may be raised. The duration of your participation if you choose to participate and remain in the study is expected to be 40 working days. The study is funded by Nomkhosi Ndaba.

The study may involve the following risks and/or discomforts participants may not be free to express themselves for fear of victimization although assurance will be given that their inputs will not be shared at all to other parties. We hope that the study will create the following benefits to participants, provide the factors that leads to the impact of Government Employees Using Biometrics will be unpacked and the participants will be able to take note of these issues and their impact during Biometrics. The researcher therefore compels all participants to take this research seriously and capture their honest opinions without any fear.

The research does not involve any potential risk, everything is expected to flow smoothly.

This study has been ethically reviewed and approved by the UKZN Humanities and Social Sciences Research Ethics Committee (approval number \_\_\_\_\_).

In the event of any problems or concerns/questions you may contact the researcher at 083 749 2177 or the UKZN Humanities & Social Sciences Research Ethics Committee, contact details as follows:

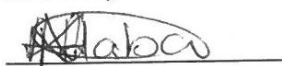
**HUMANITIES & SOCIAL SCIENCES RESEARCH ETHICS ADMINISTRATION**  
Research Office, Westville Campus  
Govan Mbeki Building  
Private Bag X 54001  
Durban 4000 KwaZulu-Natal, SOUTH AFRICA  
Tel: 27 31 2604557- Fax: 27 31 2604609  
Email: [HSSREC@ukzn.ac.za](mailto:HSSREC@ukzn.ac.za)

Your participation in the study is voluntary and by participating, you are granting the researcher permission to use your responses. You may refuse to participate or withdraw from the study at any time with no negative consequence. There will be no monetary gain from participating in the study. Your anonymity will be maintained by the researcher and the School of Management, I.T. & Governance and your responses will not be used for any purposes outside of this study.

All data, both electronic and hard copy, will be securely stored during the study and archived for 5 years. After this time, all data will be destroyed.

If you have any questions or concerns about participating in the study, please contact me or my research supervisor at the numbers listed above.

Sincerely

A handwritten signature in black ink, appearing to read 'Ndaba', is written over a horizontal line.

Nomkhosi Ndaba

## CONSENT TO PARTICIPATE

I \_\_\_\_\_ have been informed about the study entitled the impact of Government Employees using Biometrics in IT Security Management at KZN Treasury by Nomkhosi Ndaba.

I have been given an opportunity to ask questions about the study and have had answers to my satisfaction.

I declare that my participation in this study is entirely voluntary and that I may withdraw at any time without affecting any of the benefits that I usually am entitled to.

I have been informed about any available compensation or medical treatment if injury occurs to me as a result of study-related procedures.

If I have any further questions/concerns or queries related to the study I understand that I may contact the researcher, Nomkhosi Ndaba at ([nomkhosin106@gmail.com](mailto:nomkhosin106@gmail.com) or 083 7492177) or the supervisor Dr Ramluckan at [RamluckanT@ukzn.ac.za](mailto:RamluckanT@ukzn.ac.za) or 031 260 8854.

If I have any questions or concerns about my rights as a study participant, or if I am concerned about an aspect of the study or the researchers then I may contact:

**HUMANITIES & SOCIAL SCIENCES RESEARCH ETHICS ADMINISTRATION**  
Research Office, Westville Campus  
Govan Mbeki Building  
Private Bag X 54001  
Durban  
4000  
KwaZulu-Natal, SOUTH AFRICA  
Tel: 27 31 2604557 - Fax: 27 31 2604609  
Email: [HSSREC@ukzn.ac.za](mailto:HSSREC@ukzn.ac.za)

\_\_\_\_\_  
Signature of Participant

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature of Witness  
(Where applicable)

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature of Translator  
(Where applicable)

\_\_\_\_\_  
Date



## Appendix 4: Questionnaire

### INFORMED CONSENT RESOURCE TEMPLATE

#### Information Sheet and Consent to Participate in Research

Date: 18 /02 /2019

Dear Respondents,

My name is Nomkhosi Ndaba, a Masters of Commerce in Information Systems Technology Degree Student , at the Management , I.T Governance School of the University of KwaZulu Natal, with the following contact details : Cell phone number 083 7492 177 and email address : Nomkhosin106@gmail.com.

You are being invited to consider participating in a research study about

The Impact of Government Employees Using Biometrics in IT Security Management at KZN Treasury.

The aim and purpose of this research is to:

- Determine the influencing factors of KZN Provincial Treasury's decision to use biometric security.
- Determine the impact of government Employees using biometrics in IT Security Management at KZN Treasury
- Determine the impact of biometric security on work performance at KZN Provincial Treasury.
- Determine whether the implementation of biometric security has added value to service delivery.

The study is not funded by any organization and there will be no direct benefits to the participants. However, the study will enlighten the researcher with the impact of government employees using Biometrics in IT Security Management system at KZN Treasury, the influencing factors of KZN Provincial Treasury's decision to use biometric security, the impact of biometric security on work performance at KZN Provincial Treasury and whether the implementation of biometric security has added value to service delivery. The final report will be shared with participating organisation for consideration. The study requires the participants to



answer all questions honestly and fairly. The participants are also expected to indicate if they want the questions to be asked in a language that they are familiar with, ask for repeat or clarity as well as request not to answer the specific question when the participants are not comfortable to answer.

This study has been ethically reviewed and approved by the UKZN Humanities and Social Sciences Research Ethics Committee (approval number : HSS/2074/018M).

In the event of any problems or concerns/questions you may contact the researcher at 083 7492 177 or Dr Ramluckan (Supervisor) on 031 260 8854 Or the UKZN Humanities & Social Sciences Research Ethics Committee, contact details as follows:

#### HUMANITIES & SOCIAL SCIENCES RESEARCH ETHICS ADMINISTRATION

Research Office, Westville Campus

Govan Mbeki Building

Private Bag X 54001

Durban

4000

KwaZulu-Natal, SOUTH AFRICA

Tel: 27 31 2604557- Fax: 27 31 2604609

Email: HSSREC@ukzn.ac.za

Your participation in this project is voluntary. You may refuse to participate or withdraw from the project at any time with no negative consequence. There will be no monetary gain from participating in this survey/focus group. Confidentiality and anonymity of records identifying you as a participant will be maintained by the School of Management, I.T and Governance at UKZN.

I hope you will take the time to complete this survey.

Sincerely

Investigator's signature \_\_\_\_\_ Date \_\_\_\_\_

## CONSENT

I ..... have been informed about the study entitled: The Impact of Government Employees Using Biometrics in IT Security Management at KZN Treasury.

I understand the purpose and procedures of the study.

I have been given an opportunity to answer questions about the study and have had answers to my satisfaction.

I declare that my participation in this study is entirely voluntary and that I may withdraw at any time without affecting any of the benefits that I usually am entitled to.

I have been informed about any available compensation or medical treatment if injury occurs to me as a result of study-related procedures.

If I have any further questions/concerns or queries related to the study I understand that I may contact the researcher at 0834634342.

If I have any questions or concerns about my rights as a study participant, or if I am concerned about an aspect of the study or the researchers then I may contact:

**HUMANITIES & SOCIAL SCIENCES RESEARCH ETHICS ADMINISTRATION**

Research Office, Westville Campus

Govan Mbeki Building

Private Bag X 54001

Durban

4000

KwaZulu-Natal, SOUTH AFRICA

Tel: 27 31 2604557 - Fax: 27 31 2604609

Email: HSSREC@ukzn.ac.za

---

Signature of Participant

---

Date

---

Signature of Witness

---

Date

(Where applicable)

**Questionnaire for the Topic:** The Impact of Government Employees Using Biometrics in IT Security Management at KZN Treasury.

Section A: General Demographics							
1.	What is your gender						
	Female			Male			
2.	What is your Qualification						
	Matric		National Diploma		Bachelor's Degree		Post Graduate
3.	What is your position in the organization						
	User	Enrollment Officer	Management				
			Assistance Director	Deputy Director	Director		

Section B: Perceived Usefulness of Biometrics / System Quality / Information Quality									
1 = Strongly Agree		2 = Agree		3 = Neutral		4 = Disagree		5 = Strongly Disagree	
	Questions	1	2	3	4	5			
4.	Using Biometrics improves the quality of the work I do								
5.	Using Biometrics gives me greater control over my work								
6.	Biometrics enable me to accomplish the systems security control								
7.	Biometrics provides a greater organizational impact								
8.	Biometrics provides accurate information								

<b>Section C: Perceived Ease of Use of Biometrics / User Satisfaction / Individual and Organization Impact</b>									
<b>1 = Strongly Agree</b>		<b>2 = Agree</b>		<b>3 = Neutral</b>		<b>4 = Disagree</b>		<b>5 = Strongly Disagree</b>	
	Questions								
		<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>			
9.	I prefer to use Biometrics finger print as a security Management measure								
10.	I found Biometrics unnecessarily complex								
11.	I find Biometrics system easy to use								
12.	I find Biometrics as a monitoring and tracking system rather than providing security for the system.								
13.	Biometrics provide accountability for individually								

<b>Section D: Influencing Factors</b>									
<b>1 = Strongly Agree</b>		<b>2 = Agree</b>		<b>3 = Neutral</b>		<b>4 = Disagree</b>		<b>5 = Strongly Disagree</b>	
	Questions								
		<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>			
14.	Implementation of biometric security has added value to service delivery.								
15.	Using biometrics built a good impression on Employees that are using biometrics in IT Security Management at KZN Treasury								
16.	Reenrollment, enrollment of multiple fingers mitigate errors								
17.	The individuals being reliable of their actions and activities onto the system								
18.	Biometric security technology has capabilities, features, and challenges that compound the difficulty of making the decision								

Section E: Technology Used								
1 = Strongly Agree		2 = Agree	3 = Neutral	4 = Disagree	5 = Strongly Disagree			
	Questions	1	2	3	4	5		
19.	Biometrics is the latest technology that is being used for security control							
20.	KZN Treasury is using the most secured and latest technology in managing security							
21.	Using Biometrics finger print feature provides an accurate security control							
22.	The technology that is used provide a secured user identity and reliability							
23.	Using the latest technology make the user feel at ease.							

