

**A managerial framework for a secure
computerised environment in a metropolitan
municipality**

I Mofikoe



orcid.org / 0000-0003-0531-1628

Thesis accepted for the degree **Doctor of Philosophy in
Business Administration** at the North-West University

Promoter: Dr C van der Vyver

Co-promoter: Prof CJ Botha

Graduation: October 2020

Student number: 11777818

ABSTRACT

The primary objective of the study was to develop a managerial framework for a secured computerised environment in a metropolitan municipality.

The population for the study was the employees in the different entities of the CoJ Municipality (City of Johannesburg, located in the Gauteng Province, South Africa) and focused on the ICT departments and their management teams within the different entities in the municipality.

The study focused on the ICT officials within the CoJ Municipality. In total, 80 questionnaires were issued to the participants and 71 completed questionnaires were received, amounting to a response rate of 88,75%. The remaining nine questionnaires were not received back from the expected participants.

The questionnaires were returned over a period of 2-3 weeks and once completed, they were handed over to the North-West University Statistical Consulting Services (SCS) department for the capturing of data and analysis.

The conclusions of the study were based on the literature review, statistical analysis and its interpretation. Recommendations are made from the different areas of the questionnaire and industry best practices in relation to the aspects of this study.

Implications for future research in this area are also indicated with suggestions to look at the different municipalities within the country to determine how secure their computerised environment is and how lessons learned from those can be implemented in all municipalities within South Africa.

Keywords: computer security, information security, Secure computing, Secure systems, Computerised environment, Cybersecurity, ICT Policies.

EXECUTIVE SUMMARY

This Thesis comprises six chapters. Chapter 1 provides an introduction to the research, the empirical objectives as well as the research question of the study. Chapter 2 focuses on the literature review based on the major concepts of the research study.

Chapter 3 discusses the research design and different methodologies and provides a brief overview of the different research paradigms and selects the positivism paradigm and the quantitative research method for this study. The data collection instruments are identified, and interviews are discussed as means of supplementing the collection instruments and also assist with follow-up questions to participants.

Chapter 4 looks at the analysis of the data received from participants and discusses the concepts of reliability and validity in reference to the research study. For the statistical analysis, the researcher discusses frequencies, descriptives, Cronbach's alpha, Mean and Standard deviation.

Chapter 5 focuses on the development of the framework. The study provides a literature review of a theoretical framework and then look at the key ingredients that forms the framework. An explanation of how the framework was formulated is provided and the final managerial framework is presented in a graphical format with an explanation.

Chapter 6 summarises the research study process, provides the recommendations concludes this research study.

DECLARATION

I, ITUMELENG MOFIKOE, declare that the contents of this research study represent my own work and that this work has not previously been submitted for academic examination towards any other qualification at any institute of higher learning. Furthermore, the research represents my opinions and not necessarily those of the North-West University.

To the best of my knowledge and belief, this research contains no material that has been previously published or written by any other person except in cases where I have made due reference to such writers and publishers.

All possible risks that may arise related to the research study have been identified and mitigated against. I have obtained the required ethical clearance approval from the university and acknowledged my obligations and the rights of all the participants in my research study.

Signed

Date

ACKNOWLEDGEMENTS

Over the course of my research Thesis I have had the privilege to receive a lot of support and would like to thank the following people for the role they played in my journey:

- My two mothers, AK Mofikoe and Bingi, my sister Granny, and my little brothers Boitumelo & Keitumetse for the prayers and well wishes
- My two daughters, Lesedi and Lesego, and my son Itumeleng Jnr.
- My late father, MJ Mofikoe and my late son Amogelang – you'll always be in my heart and may your souls rest in eternal power
- My life partner, Tswakae Makhetha, for being a pillar of strength and always making sure that I give it my best effort no matter the circumstances
- All the other friends, family and colleagues for your support and contributions
- My two supervisors, Dr Charles van der Vyver and Prof. Christoff Botha, for your guidance and taking your time to provide the extra push I needed throughout the course of my studies
- Dr Erika Fourie from the Statistical Consultation Services at the North-West University, Potchefstroom Campus, for all the sessions and assistance with the Statistical Analysis of my research studies
- The North-West University library staff members at both the Vaal Triangle and Potchefstroom campus for all the assistance with journals, articles, textbooks and all the relevant material required for my studies
- The ICT officials from the different entities within the City of Johannesburg for taking time out of their schedules to participate in my research studies
- The CIO forum in the City of Johannesburg and the City Manager, for the request and authorisation to do my research studies within CoJ.

TABLE OF CONTENTS

ABSTRACT i

EXECUTIVE SUMMARY ii

DECLARATION iii

ACKNOWLEDGEMENTS iv

TABLE OF CONTENTS v

LIST OF TABLES x

LIST OF FIGURES xi

LIST OF ACRONYMS xii

CHAPTER 1: ORIENTATION AND PROBLEM STATEMENT 1

1.1 INTRODUCTION 1

1.2 PROBLEM STATEMENT 1

1.3 OBJECTIVES OF THE STUDY 3

1.3.1 Primary objective..... 3

1.3.2 Secondary objectives..... 3

1.3.3 Empirical objectives 3

1.4 RESEARCH QUESTIONS 4

1.5 RESEARCH DESIGN METHODOLOGY 4

1.5.1 Research Paradigm 4

1.5.2 Research Methodology 5

1.5.3 Literature Review..... 7

1.5.4 Empirical study	8
1.6 ETHICAL CONSIDERATION	9
1.6.1 Limitations of the study	10
1.7 CHAPTER DIVISION	11
1.8 CONCLUSION	13
 CHAPTER 2: LITERATURE REVIEW ON A SECURED COMPUTER ENVIRONMENT	14
2.1 INTRODUCTION	14
2.2 DEFINING MAJOR CONCEPTS	15
2.3 OVERVIEW OF A SECURE COMPUTERISED ENVIRONMENT	18
2.4 PROTECTING THE ASSETS OF THE MUNICIPALITY	21
2.5 INFORMATION SECURITY	23
2.6 SECURE TECHNOLOGY PLATFORMS AND CHANNELS	26
2.7 SECURE SYSTEMS	28
2.8 CYBER SECURITY	31
2.9 ICT POLICIES	33
2.10 CONCLUSION	35
 CHAPTER 3: RESEARCH DESIGN AND METHODOLOGIES	36
3.1 INTRODUCTION	36
3.2 DIFFERENT RESEARCH PARADIGMS	36
3.2.1 Positivism.....	38
3.2.2 Interpretivism.....	39
3.2.3 Critical Social Theory.....	40
3.3 RESEARCH DESIGN AND METHODOLOGY	41
3.3.1 Qualitative research	43

3.3.2 Quantitative research	44
3.3.3 Mixed methods	45
3.4 POPULATION AND SAMPLE	47
3.4.1 Population	47
3.4.2 Sample and sampling method.....	48
3.5 DATA COLLECTION METHODS	51
3.5.1 Questionnaires	51
3.5.2 Interviews	52
3.6 CONCLUSIONS	57
CHAPTER 4: DATA AND ANALYSIS	58
4.1 INTRODUCTION	58
4.2 PURPOSE OF THE STUDY.....	58
4.3 DATA COLLECTION INSTRUMENT.....	59
4.3.1 Procedure for data collection.....	60
4.3.2 Ethical consideration	60
4.3.3 Limitations of the study	61
4.4 RELIABILITY AND VALIDITY	61
4.4.1 Reliability.....	61
4.4.2 Validity.....	61
4.5 STATISTICAL ANALYSIS	62
4.5.1 Frequencies	64
4.5.2 Descriptives	67
4.5.3 Cronbach's alpha, mean and standard deviation.....	77

4.6 CONCLUSIONS	83
CHAPTER 5: FRAMEWORK FOR A SECURED COMPUTERISED ENVIRONMENT	84
5.1 INTRODUCTION	84
5.2 A FRAMEWORK FOR A SECURE COMPUTING ENVIRONMENT	85
5.3 DEVELOPMENT OF THE FRAMEWORK	88
5.3.1 Theoretical framework	88
5.3.2 ICT department's role.....	90
5.3.3 Level and type of skills required	91
5.3.4 Software	94
5.3.5 Hardware	95
5.3.6 Applications	96
5.3.7 ICT governance.....	98
5.3.8 ICT Strategy	102
5.3.9 Formulation of the framework.....	103
5.4 THE MANAGERIAL FRAMEWORK.....	105
5.5 CONCLUSIONS	106
CHAPTER 6: RECOMMENDATIONS AND CONCLUSIONS	108
6.1 INTRODUCTION	108
6.2 PRIMARY AND SECONDARY OBJECTIVES	108
6.2.1 Primary objectives.....	109
6.2.2 Secondary objectives.....	109
6.2.3 Empirical objectives.....	109

6.2.4 Research questions	109
6.3 LIMITATIONS OF THE STUDY	110
6.4 SUMMARY OF THE STUDY RESULTS.....	111
6.5 RECOMMENDATIONS	114
6.6 INDICATIONS FOR FUTURE RESEARCH.....	116
6.7 CONCLUSION	117
REFERENCE LIST.....	118
APPENDIX A: SURVEY QUESTIONNAIRE.....	138
APPENDIX B: RESEARCH ARTICLE.....	145

LIST OF TABLES

Table 2-1: ISO Standards Security Controls	25
Table 3-1: Strength and weaknesses of semi-structured interviews.....	55
Table 4-1: Analysis on personal awareness of computer related issues.	68
Table 4-2: Analysis of security audits within the municipality	72
Table 4-3: Analysis of management related questions	75
Table 4-4: Cronbach alphas and descriptive statistics of factors	78
Table 4-5: Independent T-test and Man-Whitney for Ethnicity	79
Table 4-6: Independent T-test for Age Group	80
Table 4-7: Independent T-test for Experience Group.....	81
Table 4-8: Independent T-test for Qualification Group.....	82
Table 5-1: Municipal's entities requirements for hardware	95
Table 5-2: Municipal's entities requirements for Applications	96
Table 5-3: ICT Governance Policy Framework	100
Table 5-4: Research questions and groupings	104

LIST OF FIGURES

Figure 2-1: 3 Pillars of Cyber Security	14
Figure 3-1: Different research paradigms	37
Figure 3-2: Factors affecting the choice of a Research Paradigm	37
Figure 4-1: Gender statistics	64
Figure 4-2: Ethnicity	65
Figure 4-3: Age grouped.....	66
Figure 4-4: Qualification Grouped	66
Figure 5-1: Unknown source	99
Figure 5-2: The Managerial Framework.....	105

LIST OF ACRONYMS

AR - Action Research

ASW – Australian Social Work

CIA – Confidentiality Integrity and Availability

CoJ – City of Johannesburg

CSIR – Council for Scientific and Industrial Research

DCS – Distributed Control Systems

DoS – Denial of Service

ECP – Electronic Communications Policies

EI – Energy Internet

EU – European Union

GDP – Gross Domestic Product

GPS - Global Positioning Systems

ICS – Industrial Control Systems

ICT - Information and Communication Technology

ICTD – Information and Communications Technology Development

IDS – Intrusion Detection Systems

IoT – Internet of Things

IS – Information Security

ISA – Information Security Awareness

ISP – Information Security Policies

ISRM – Information Security Risk Management

IT – Information Technology

NDIS – Network Detection Intrusion Tools

NGO – Non-Government Organisations

R&D – Research and Development

SCADA – Supervisory Control and Data Acquisition

SIEM – Security Information and Event Management

SMEs – Small and Medium-sized Enterprises

SOC – Security Operations Control

SSL – Secure Socket Layer

TeG – Transformational e-Government

TMIS – Telecare Medical Information Systems

UN – United Nations

CHAPTER 1: ORIENTATION AND PROBLEM STATEMENT

1.1 INTRODUCTION

Computing platforms are becoming more difficult each day, and as a result, aspects of security require improved defensive solutions. The situation leads to reasoning that structural engineers would never accept, such as claiming that obviously weak systems are 'strong' simply because we are ignorant as to which specific elements will fail (Kocher, 2016:22).

Despite the progress (redesign and strengthening security programs) made in the security of traditional distributed systems, the securing of the computing systems poses new challenges due to the dynamic nature of such systems, e.g. topology not fixed, wireless network and the computation is context aware. Security requirements are highly dependent on dynamically changing contexts such as user activity, location, nearby people and available resources (Siewe, 2016:121).

To increase the trustworthiness of the computing environments, a dependable approach to system development must be followed, which ensures that all the aspects of how that system can securely function are addressed.

1.2 PROBLEM STATEMENT

The City of Johannesburg has recently been in the process of rolling out free Wi-Fi technologies across the Johannesburg Metro Municipality in a bid to improve its service delivery and interaction with its customers. The city views its the technology investments as a catalyst to improving the different ways in which it can interact with the customers by putting in place a secure computerised environment that will enable a better service offering, interaction and improved service delivery to the residents of the Municipality.

A lot of technologies within CoJ are old and as a result they are unable to provide efficient and effective customer service to their customers. The City therefore has to ensure that it has the necessary technologies and systems in place that will ensure that their computerised environment is able to provide its customers with an improved customer experience in their contact with the municipality.

Municipalities are often trapped in a vicious cycle of under resources and economically stressed to facilitate the desired levels of service and infrastructure. The poor municipal services are often attributed to the significant ICT deficits which affect overall governance, planning and resource mobilisation and thus the municipal sector requires innovative ways of providing and accelerating the delivery of municipal services (Joseph & Ogra, 2013:26).

According to (Adonis, 2018:261), it is a legal requirement that every municipality must establish a performance management system. This performance management system must be in line with the priorities, objectives, indicators and targets contained in the municipal Integrated Development Plan. The following aspects constitute the core components of the municipal performance management system:

- Key performance indicators (KPIs) that will serve as a yardstick for measuring performance with regard to the municipality's development priorities.
- Measurable performance targets with regard to the identified development priorities and objectives.
- Monitoring of performance.
- Measurement and review of performance.
- A process of regular reporting to the municipal council, the public and appropriate organs of state.

In their study in the United Kingdom, Thales UK Ltd (2013:2) discovered that more companies are expected to come into contact with the threat of losing their confidential information through cybercrime. The number of breached companies in 2013 amounted to 93% of large companies with 87% of the small growing businesses having been victimised by cybercrime. These attacks normally result in significant revenue losses and in some cases the total collapse of the business operations.

With the advent of technology and more businesses investing in Information and Communication Technology (ICT) to enable their business, secure computing environments require specific focus and attention. Globalisation, the speed with which we do business and the mobility which the different technology platforms provide, mean that an organisations' competitive edge and survival can be determined by the type of technology it has in place to conduct its business.

The challenge stems from the fact that technology has become part of our daily lives, and the majority of customers are becoming sophisticated from their improving interactions with technology in their everyday lives. With the gap in the digital divide closing, more people in societies are engaged on smartphones, tablets and have an online presence.

Services such as Wi-Fi connections, self-help facilities and the enablement of e-government services to citizens and communities, increase the risk profile on the security of the information used/consumed on these platforms. Cybercrime is now the fourth most reported economic crime in South Africa. The South African economy reportedly loses R1 billion each year due to online criminal activities (Food Review 2018).

The City of Johannesburg's Integrated Development Plan (IDP) 2019/2020 review shows how the municipality aims at intensifying efforts to deliver on its mandate. While the city acknowledges the mountainous challenges that remains before the municipality, it continues to tackle the its challenges and unite behind the common goal of building a Johannesburg that works for all its residents (IDP 2019/2020 Review).

1.3 OBJECTIVES OF THE STUDY

1.3.1 Primary objective

The primary objective of the study is to provide a managerial framework for a secure computerised environment in a metropolitan municipality.

1.3.2 Secondary objectives

To ensure that the primary objective is addressed, the following secondary objectives have been formulated for the study:

- Explore the role of the ICT department within the municipality.
- Determine the types of ICT skills required amongst the employees within the municipality.
- Explore the governance and framework applicable to the municipality.

1.3.3 Empirical objectives

In accordance with the primary objective of the study, the following empirical objectives have been formulated:

- To provide input through research on how an organisation can ensure that its computerised environment is secured.
- Provide an overview of the 'best practice' levels required for a secure computerised environment in the workplace.

1.4 RESEARCH QUESTIONS

From the above-stated objectives, the following research questions were formulated.

- What role does the ICT department play within that organisation and how does it compare with other similar organisations?
- Which are the required levels of skills and education as well as the most appropriate organisational structure?
- What are the required/most suitable types of software, hardware and applications?
- Which legislative requirements or governance is in place to address the secure computerised environment?
- What strategies can be put in place to deal with challenges posed by a computerised environment?

1.5 RESEARCH DESIGN METHODOLOGY

1.5.1 Research Paradigm

Educational research is a systematic activity that is directed towards providing knowledge or adding to the understanding of existing knowledge which is of relevance in order to improve the effectiveness of education. Research students generally make use of words such as systematic, knowledge, understanding, existing and improving needs to be understood beyond their surface meaning (Dammak, 2015:1).

The words mentioned above provides further emphasis in research when they are deeply interpreted, and therefore, a reflection and an understating of these words will provide one with the ability to differentiate between the different research paradigms.

The researcher needs to ensure that the most appropriate research techniques are used in their research process mainly to ensure that knowledge is gained on the subject and more profound understanding and contributions can be made to the existing body of knowledge.

Cronje (2014:1) argues that researchers should be familiar with arguments originating from the various paradigmatic stances, that paradigms and philosophies should not lead the initial enquiry but should instead inform results obtained. Plainly stated, research should not be steered by a chosen paradigm.

For any researcher to attain their stated purpose, they need to embark on a literature and quantitative empirical study. The literature study, in general, is intended to provide a conceptual framework for contextualising the research and informing the empirical part of the study (Lombard & Kloppers, 2015:1)

Fonseca (2013) identifies design flaws emanating from poorly formulated research questions, a poor approach to answering the research question, the choice of a weak or unreliable method, choice of an incorrect method or model for the problem to be studied, type or size of the chosen sample, inappropriate statistical analysis and/or unreliable or incomplete data.

1.5.2 Research Methodology

Agee (2009:431) explains the theory of Habermas on how researchers typically view a question as a beginning point of their research. Once a satisfactory question is in place, the study can begin. Though a research question fulfils this function, much more should be involved in creating and using research questions in qualitative studies. The reflective and interrogative processes that are involved in developing research questions can give shape and direction to a study in ways that are often underestimated.

Good questions will not necessarily produce good research, but if poorly constructed, questions will likely create problems which will have an impact on all the different stages of the study. Ultimately, the quality of the initial question impacts whether or not a study is approved by a dissertation committee, published or funded.

The methodology of action research (AR) was situated within the socio-critical paradigm in the 1920s and was developed within the 1940s and in particular the 1970s in the area of educational research. The one thing that set apart the AR of the 1970s to the previous ones was its rejection of a methodology oriented towards positivist (objective) research but promoted interpretive (subjective) research (Gomez *et al.*, 2017:186).

Kemmis (2010:417) argues that the primary justification of AR is that it makes a direct contribution to transformative action as well as changing history, meaning that the first concerns for action researchers should be the contribution of their action to history and not necessarily theory.

The strength of the practice-oriented research strategy is to develop knowledge about the improvement of practices. The main goal of practice-oriented research is that it focuses on research that comes from the professional practice and in which the knowledge created in the research contributes directly to this professional practice (Hermans & Schoeman, 2015:26).

The use of case studies as a research method continues to gain mainstream acceptance in both the entrepreneurship and information systems research to develop conceptual and theoretical models that are novel but very much grounded in literature. Even with the availability of many texts on the case study method and its growing in acceptance and use thereof, there are still relatively few examples that discuss how the case study method can be applied (Ponelis, 2015:535).

Reischauer (2015:279) suggests a combination of qualitative methods, artefact analyses, semi-structured qualitative interviews and participant observation to study the research topic. He emphasises that first-order concepts are constricted by using qualitative content analysis to analyse the data separately. Combining these separate concepts with the constant comparison technique will then create second-order concepts and therefore a comprehensive understanding of the concept under research.

Sykes *et al.* (2016:319) explain that research begins with the formulation of a clear question, the collection of evidence focused on the specified problem, analysis of the results which is followed by an appraisal of their validity (how close to the truth) and relevance (importance and usefulness). In order to achieve this, the study design needs to be appropriate for the specific problem, bearing in mind the levels of available evidence.

According to Laher (2016:316), the description of the design flaws and originality requirements support the view that the criteria of internal/external validity and reliability are core to a rigorous quantitative study.

1.5.3 Literature Review

According to Waggett (2013:1), passwords are the preferred, but sometimes difficult way, to keep personal data safe. Trying to pick a term that is easy to remember would probably be easy to foil as many users often battle with their own passwords which are supposedly tough to crack.

It is essential for users of computer applications to be aware of their personal vulnerabilities related to their use of the internet. Users often do not think about the security (or lack thereof) of commonly used technology, such as the global positioning systems (GPS) on their cell phones or the information in their digital health records. All across the world, interest in cybersecurity, particularly for governments and organisations, remain high (Gay, 2011:68).

Computer security educators around the world (universities, colleges and other institutes) have designed courseware with hands-on laboratory exercises for computer security courses, but a lot of those do not have a specific focus on secure web development. Textbooks on web security that are suitable for undergraduate courses are very limited. These textbooks, published in recent years, only have a chapter or section on web security with a limited overview of secure socket layer (SSL) and certificate authority (Chen & Tao, 2012:39).

Parker (2012:388) emphasises that the concept of cloud computing eludes its precise definition, as the underlying technology continues to evolve quickly. He further argues that the term has become more one of branding and marketing than a useful descriptor of any particular technological system.

Cloud computing is the most significant emergence in information technology circles in recent times. It is a model that saves costs and provides increased efficiency with the possibility of widespread use of economies of skills and scale.

Government agencies and industries can be empowered by the use of ICT to provide efficient and transparent services to citizens. This enables the implementation of new ways of delivering services to citizens, industries and other government agencies. In other words, the information society is continually redefining the way that public officials should operate to change the mechanisms of service delivery (Joseph & Olugbara, 2017:1).

1.5.4 Empirical study

The empirical study comprises the following methodology measurements.

1.5.4.1 Target population

The population for the study were the employees in the different entities of the City of Johannesburg (CoJ) Municipality. Other data records were gathered from the systems, files and other applicable documents that govern information security within the Municipality.

1.5.4.2 Sampling frame

This study focused on the ICT departments and their management teams within the different entities in the Municipality (CoJ, located within the Gauteng Province, South Africa).

1.5.4.3 Sample method

The sample design is a well-recognised issue in social research, and as many kinds of literature on research convey, the success of any empirical study rests to a large extent on the adequacy and accuracy of the sample in order to ensure that the research objectives and aims are addressed (Uprichard, 2013:1).

The following two different types of random sampling were used in this study:

- Population – ICT departments within the City of Johannesburg (CoJ).
- Simple random sampling technique to select members of each entity to participate in the study.

1.5.4.4 Sample size

The sample size of the study comprised of the ICT department's municipal entities within CoJ. The sample size of the study comprised of at least 50 questionnaires from the Municipality.

1.5.4.5 Measurement instrument and data collection method

The research on the described objectives were based on the literature review and an empirical study. A quantitative research methodology was used in the form of a questionnaire that was administered to the employees of the organisation to gain their insight and perspective on how secure they believe their computerised environment is.

Interviews were also conducted with the ICT department officials to determine the level of security within their environment, third parties such as service providers were also contacted as well in cases where some of the internal functions of the City are outsourced.

1.5.4.6 Statistical analysis

In this research, questionnaires were administered to the participants of the study as the means of data collection. Interviews were used to validate specific responses and to obtain additional information. Responses from the participants were analysed and interpreted, first to ensure that they address the problem statement and objectives and secondly, to provide a detailed view on the status quo of the computerised environments within the different entities.

According to Ali and Bhaskar (2016:662), statistics is a branch of science that deals with the collection, organisation, analysis of data and drawing of inferences from the samples to the whole population. A proper design of the study is required with an appropriate selection of the study sample and the choice of a suitable statistical test. Adequate knowledge of statistics is necessary for proper designing of a research study and the use of improper statistical methods may result in erroneous conclusions which may lead to unethical practice.

1.6 ETHICAL CONSIDERATION

According to Ketefian (2015:165) guidance is required in research for the protection of vulnerable groups or individuals who are least able to take steps to protect themselves. Greater vigilance is required on the part of researchers to ensure that oversight and precautions are in place against vulnerable individuals.

In relation to my study, the following considerations were taken into account:

- **Plagiarism** – the researcher did not undertake other people's work and represent it as my own. Where other researchers have been cited, they are acknowledged as such.
- **Research approval** – the research was approved in accordance with all the rules and regulations as specified by the University colloquium.
- **Professional conduct** – all the details of the participants as well as the information collected were treated as private and confidential and are used for the purpose of this research.

All participants in this research participated at their own free will and were required to sign the consent form. The consent form provided participants with the background of the research and its intended purposes in order to inform the participants of their roles and contribution to the research. Participants had an option to take part or not to take part in the research.

1.6.1 Limitations of the study

The study was limited to the information that was gathered through questionnaire responses from the participants. Articles, textbooks, journals and other thesis and documentation available in relation to the topic were consulted.

The following factors had an impact on the data available for the statistical analysis:

- Non-participation from the target group
- Management not providing all the required information
- Participants not responding to the questionnaires & interviews with honesty

All means possible were undertaken to ensure that the information required and received was adequate enough to draw conclusive and informative findings from the research. Mitigations on our limitations are further outlined and explained in Chapter 6 prior to the formulation of our research recommendations.

1.7 CHAPTER DIVISION

The breakdown of chapters in the thesis is as follows:

Chapter 1: Introduction and the problem statement

Chapter one provides us with an overview of the entire research study. The chapter begins with an introduction and then the problem statement is explained in detail. The research focus is identified with the different research objectives, the research design methodology and the chapter conclude with the limitations on our research study and the breakdown of the different chapters within our research study.

Chapter 2: Literature Review

Chapter two focuses on the literature review. The major concepts of the research study are defined with a view from the different sources and further explained in the context of their contribution in building our framework. The chapter also provides an overview into what is meant by a secure computerised environment and what measures can be taken to ensure that the assets of the municipality are protected from a technology point of view.

Chapter 3: Research Methodology

Chapter three focuses on the research design and the different methodologies that can be followed. The different research paradigm are identified and explained in detail – the choice of the positivism research paradigm is articulated in reference to our research study. The different research designs are also identified, explained and the choice for our research study clarified but also indicating how more than one research methodology can be used or a combination of the qualitative and quantitative methods.

The research sample, population as well as the different sampling methods are explained. The chapter concludes with the identifying the data collection method, which is our questionnaire and how it will be supplemented with interviews as the different interview techniques are discussed.

Chapter 4: Data and Analysis

Chapter 4 provides an overview on the analysis and interpretation of the data that was collected during the research process. The purpose of the study is discussed, and we explain in detail the data collection instrument and how the process was administered in relation to the participants of our research study.

The ethical considerations of the study are stated and potential limitations to our research are included. The reliability and validity of our research is explained, and all key areas of our statistical analyses are explained and the interpretation thereof in relation to our data is completed.

Chapter 5: Framework for Secure Computing Organisation

Chapter five of our research study focuses on the framework that we are developing for the City of Johannesburg Municipality. The theoretical concept of the framework is explained in relation to the formation or development of a framework for a secure computerised environment in a municipality

From the research objectives and questions, all aspects that should be considered in the formulation of our framework are discussed in detail, with emphasis on how they will contribute and what their expected output should be in relation to the entire research study. The managerial framework's development path is clearly articulated.

Chapter 6: Recommendations and Conclusions

Chapter 6 focuses on the recommendations and then concludes our research study. The chapter focuses on the link between our research objectives, literature review, statistical analysis and the development of the framework in the previous 5 chapters in response to our problem statement.

The mitigations in relation to the limitations of our study are outlined and the overview of the study results is provided. The recommendations of the research study are documented and the chapter concludes with the indication of potential research studies that can be done in this field.

1.8 CONCLUSION

Chapter one details the overview of the study and the layout together with the approach that was followed in the study. A brief description of the different computer platforms and their security concerns is provided and how those can be addressed to ensure a secure computing environment for an organisation.

In this Chapter, the problem statement of the study was identified, the objectives of the research which give rise to the research questions and then define the research methodology followed in the study. Ethical considerations and any limitations to the study were also addressed.

Organisations of the modern era now consider the value of Information and Communications Technology (ICT) as the mechanism that allows them to create and maintain their competitive edge in both the physical and virtual marketplace. Nonetheless, given how Information Technology (IT) has become a key driver for many businesses, the information security breaches and risks that can exploit an organisations' technical and human behaviour poses a serious threat to the day-to-day running of any organisation (Hsu *et al.*, 2012:918).

It is important to note that as the organisations begin to compete in the global space and mature in their IT infrastructure and reliance on IT, this is likely to increase their risk in information security breaches. Organisations need to ensure that they have both the required technical and human skills required to ensure the safety of their organisations' computer environment.

The main objective is to provide a managerial framework for a secure computerised environment in a metropolitan municipality.

The next chapter in our research study focuses on the literature review, the definition of the major concepts as well as the overview of what is meant by a secure computerised environment in metropolitan municipality.

CHAPTER 2: LITERATURE REVIEW ON A SECURED COMPUTER ENVIRONMENT

2.1 INTRODUCTION

The aim of this chapter is to provide a broader understanding of the theoretical literature available on secure computing environments and the factors, such as information security, secure systems, cybersecurity and legislation, that make up this environment from both a technical and human perspective.

Even with the right for citizens in place for them to be able to access information, government institutions also have an obligation to ensure the security of such information in their endeavours to draw a balance between freedom and accessibility. The rights of the individuals that require access to information should always be balanced against those who are tasked with the responsibility of protecting and providing the required information.

The business of securing computers, networks and the companies that use them is alive and well. Opportunities exist for information security professionals in corporate environments, security product vendor environments, government, military, educational institutions and professional services firms.

The words 'cybersecurity' may bring to mind international terrorism, corporate privacy and national security issues on all three spheres of government, however cybersecurity spans much more.

A cyber security environment is always dependent on three pillars which ensure that a computerised environment can be secure. These three pillars are policy and procedures, technology, and people, as depicted in Figure 2-1.

Cyber Security		
<i>Policies and Procedures</i>	<i>Technology</i>	<i>People</i>

Figure 2-1: 3 Pillars of Cyber Security

2.2 DEFINING MAJOR CONCEPTS

The right of access to information is a component of the broader right to freedom of expression recognised in basic instruments of the United Nations (UN) and regional human rights systems. The right of access to information has further gained recognition as a stand-alone right guaranteed in constitutions and other laws. It imposes a duty on governments to facilitate access of everyone to information that is held by public institutions in a manner that is both accessible and can be retrieved irrespective of how it was produced (Salau, 2017:368).

Snyder (2012:25) argues that job security is nothing like it was a few years ago, however, there is one sector of IT that is providing challenging and well-paying career opportunities. Every time a new computer technology is created, it creates a new avenue for cybercriminals and pranksters to potentially infiltrate a computer solely for the purposes of wreaking havoc or stealing of personal information, intellectual property or customer data.

Each and every field, from medicine, education or finances to online shopping are affected by the need to ensure that personal, institutional and corporate information is protected and that those who are active on the internet do not fall victim to predators and scammers. Internet security has taken on a new meaning, also having to include domestic and international intelligence related to protection and defence (Gay & McCoy, 2012:46).

The Internet of Things (IoT) brings the risk inherent in potentially unsecured information technology systems into homes, factories and communities. IoT devices, networks, or the cloud servers where data is stored, can be compromised in cyber-attacks if the devices are not secured (GAO Reports, 2017:1).

An independent study on cybercrime by the computer security company McAfee in 2014, estimates that cybercrime costs South Africa around R5.8 billion per annum, which equates to 0.14% of the country's Gross Domestic Product (GDP). Cybercrime is not only limited to large organisations and business institutions but also extends to individual users of the Internet. A 2013 report by Symantec estimates that over 1 million South African citizens fall victim to cybercrime each year, ranking the country third on the list of countries hardest hit by cybercrime (Mcdonald, 2015:47).

Computer security - The ability to provide critical business services on the Internet and using technology, efficiency and convenience associated with the technology as well the ability to ensure that proper safeguards are in place (Duffy, 2011:21).

Computer security – Combating the threat of security incidents from employees (current and former) – often related to carelessness or human error (Veiga, *et al.*, 2020:2)

Computerised environment – organisations are increasingly capturing data about their customers, which enables them to analyse and understand them better and understand which enables them to offer custom products and services. This environment includes the growing number of devices with data, such as cell phones and tablets (Visser, 2015:26).

Computerised environment – anything or many things that cooperate with each other, connect to the Internet, generate any data, provide any service to any user and enable him to access these services and data from anywhere and at any time by any possible or available means (Abi Sen & Basahel, 2019:1)

Cyber security – the ability to perform both reactive and proactive functions to help protect and secure critical information technology assets of an organisation or even the country (Gcukamana, 2009:47).

Cyber security – the unavoidable trends of higher number of generation systems and increased complexity of control systems results in higher cybersecurity risk across the board for renewables and the need for a strategic approach for management of renewable facilities across the nation (Pack, 2019:1)

ICT policies – a set of rules and guidelines for organisations to provide an efficient and safe information-sharing platform that can be consumed by the users who access the systems (Yoon, 2017:2).

ICT policies – Information and Communication Technology (ICT) policy is “an integrated set of decisions, guidelines, laws, regulations, and other mechanisms geared to directing and shaping the production, acquisition, and use of ICT’s (Kunyenje & Chigona, 2019:2).

Information security – the ability to preserve the confidentiality, integrity and availability of information in an organisation.

Information security – An organisation's success or failure in implementing information system security depends on the actions of its employees and how risky they behave online (Nel & Drevin, 2019:146)

Municipalities – the administrative body of governments, which is responsible for the provision of basic services such as water, electricity and waste management to the citizens.

NGO (non-government organisations) - civil society actors who play an increasingly important role by offering a voice for the disenfranchised through their advocacy and a helping hand for the disadvantaged through their operations (Chesterman, 2018:159).

NGO (non-government organisations) - two common characters are social purposes and dealing with the constraints on the distribution of surplus (Cordery, *et al.*, 2019:1).

Secure computing – a value chain in an organisation where organisations' systems must be tightly secured, and clear rules developed around data ownership, access and destruction (Young, 2016:33).

Secure computing – often referred as the ability to capture, store and process data by making use of large computing and storage resources.

Secure systems – to ensure that the system or application will be available for use and that it will deliver uncorrupted information (Landwehr, 2001:3).

Secure systems – the provision of services using mobile communication technology and context aware technology which can be remotely accessed at any time (Sareen, *et al.*, 2017:1437).

2.3 OVERVIEW OF A SECURE COMPUTERISED ENVIRONMENT

Dysart (2013:31) offers the following computer security tips that employers can put in place in their organisations:

- make security training ongoing;
- use emails (inbox) for regular security tips;
- ensure that you have the buy-in of all the employees;
- constantly remind everyone in the organisation about ethical issues; and
- provide constant education on security and cyber threats.

Attackers are developing sophisticated ways and means of avoiding detection based on the vulnerabilities in software and weak configuration of technical security countermeasures. Examples of security countermeasures include Network Intrusion Detection Systems (NDIS) which are capable of performing fine-grained network data and protocol-level analysis to identify anomalous and malicious traffic; and anti-virus tools that scan incoming software and attempt to match code signatures to a list of known malicious code bases (Burnap *et al.*, 2018:400).

Cloud computing has emerged as the latest and most popular development in information technology. Observers believe that it represents a breakthrough development that has the potential to transform the nature of computing as a whole fundamentally. The opposite view though is that it is nothing more than an over-hyped repackaging of already extant technologies (Yoo, 2011:406).

The new IT paradigm of cloud computing offers considerable advantages in terms of installations, configuration, updating, compatibility, costs and computational power, and in the last few years cloud computing has already provided enormous benefits to a number of organisations. However, it also comes with a number of potential risks.

The year 2010 witnessed a huge cyber-attack on the popular cloud email services of Gmail, and the sudden discontinuation of cloud services to WikiLeaks by Amazon. Other issues followed in 2013 with the NSA spying scandal, the 2014 nude photo iCloud hack and the Sony hack. Apparently hackers are increasingly turning their attention to the cloud computing services (de Bruin & Floridi, 2017:22).

Internet users who are visually impaired are more vulnerable to cyber-attacks due to the absence or limitations of visual cues, inaccessibility of visual cues, and the lack of software support to inform the users about the potential cybersecurity threats. With challenges posed by the design of web pages, users who are visually impaired are confronted with other security challenges when surfing the web, login sessions & timeouts, security updates, malware and phishing (Inan *et al.*, 2016:29).

Developing countries such as South Africa, Zimbabwe and Nigeria are often the target of cybercrimes due to their weak control and security measures. For example, in South Africa the National Cyber Security Hub (CSIR, 2016) reported that there were 6 000 attempted cyber-attacks against South Africa's critical infrastructure, business and internet service providers between 2011 and 2015. There were also an additional 6 000 attacks recorded that related to phishing incidents (Mpuru, 2017:44).

Okesola *et al.* (2016:1) notes that Nigeria had the largest Internet population in Africa at 11th position in the world as of October 2013. Also, 'social networking' was in the second spot (72%) of activity on the Internet after 'news and information' (78%). By June 2015, Nigeria had 15 million monthly active users, all of them using mobiles to like, share and upload content on social networks.

In South Africa, the Johannesburg Metropolitan Council has substantially heightened its security with the implementation of the First National Bank's (FNB) 'Smartbox' systems at numerous points throughout the region. These Smartboxes act as effective deterrents against robberies and in addition to greater security, they offer other benefits which include cost savings, quicker identification of forged or mutilated banknotes and the potential elimination of shortages between the cashier points and the bank (Marais, 2003:126).

Abroad, the US Government spends upwards of \$81 billion annually on its IT systems, components, software and related services, and it is highly reliant on IT to perform its many functions and responsibilities. This technological necessity is due to their recognition of a multitude of direct and indirect security threats against the governments IT systems (Morrison, 2013:750).

In Europe, according to Sorrentino *et al.* (2017:707) the digital agenda (especially e-government policies) is one of the seven pillars of the Europe 2020 Strategy, which was launched by the European Commission in 2010 to set the goals and timeframes for the economic growth of the European Union (EU). The Digital Agenda pushes EU member-states to embrace ICTs, including digital television and mobile telephony. The plan is described as a significant game-changer in that it requires each EU member-state to design and implement a strategic plan, identify priorities and methods of intervention, and align their targets to those set by the European Commission for the entire EU.

To ensure a secure computing environment, security systems designers need to choose different approaches to achieve the overall security improvements of systems or to mitigate the impact of specific types of attacks on their computing environments. How much an environment is intrusion tolerant means to what extent does it provide the minimum level of safe operations when facing unexpected intrusions (Lee et al., 2018:653).

According to Okurumeh and Ukaoha (2015:228), social media has been commonly used throughout the world to voice objection about government plans and organising of protests which have brought down the government in Morocco, Egypt and created a ripple effect in Bahrain, Saudi Arabia and Syria. Social media has presented varieties of new threats posed by cybercriminals, especially where the websites are vulnerable to security breaches.

The emergence of social technology/computing also poses security risks to many of its users. More people are building communities online and remain in contact with users and organisations at any time. Users are able to make statements about any issues on Facebook, Twitter, Myspace and other platforms available in social computing.

2.4 PROTECTING THE ASSETS OF THE MUNICIPALITY

Protecting the assets of the organisation is the responsibility of management. Assets include sensitive information, such as product plans, customer records, financial data, and the IT infrastructure of the organisation. Security measures are often in place to restrict members of the organisation in their working patterns, and there may be a potential temptation to flout security rules. This typically happens when the security instructions within the organisation do not come from a superior authority but from some other branch of the organisation (Gollman, 2011:15).

Wempen (2014:542) emphasises that computer crime is becoming increasingly common and it is relatively easy to attack computers in order to cause disruptions or steal data. Because of the ease with which attacks can be launched, it is essential that organisations remain aware of security and then take the necessary steps to secure their data and online identity. Computer security is built around upholding three primary goals, i.e. confidentiality, integrity and availability. This means the following:

- **Confidentiality:** Data should be visible and accessible only to those who are authorised to see it.
- **Integrity:** Information that you see and store should be reliable, accurate and should not be tampered with. The information should be trusted.
- **Availability:** Information should be accessible at any time, and from anywhere including after a mishap or a disaster.

Salomon (2006:5) identifies the seven classes of computer security and crime as follows.

- **Insiders overt:** overt actions by insiders are often performed by disgruntled employees and result in the destruction of data and equipment.
- **Insiders covert:** generally speaking, insiders have more information about a place of work than outsiders, which is why they can wreak havoc.
- **Insiders unintended:** employees can make errors and can also neglect their duties.
- **Outsiders overt:** physical attacks on computers and network facilities can also be referred to as Denial of Service (DoS).

- **Outsiders covert:** this class consists of the various types of rogue software sent from the outside to a personal computer or to a large computer facility.
- **Outsiders unintended:** it is very rare that an outsider will harm a computer or data unintentionally.
- **Accidents:** they always happen, not only in the computing field. They can be caused by nature (earthquake/floods) or indirectly by humans.

The development of communication technology provides efficient services based on sustainable infrastructures that improve the human quality of life. As smart devices, such as smart-phones, smartwatches, and tablets become widely available, it has become possible to access various services and to allow people to utilise information at any time and from anywhere. Added to that is the ubiquitous smart society, in which the combining of the data from smart devices and sensors enables intelligent communication (Lee *et al.*, 2017:1).

Technology has become an essential tool for many non-governmental organisations (NGOs) and groups collecting data in the developing world. Technology has the ability to provide people in remote regions with access to information and allow organisations to collect vital information within the communities that they serve. Information and Communication Technology for Development (ICTD) is the study of what technology can accomplish and how it can be used in low-resource settings around the world. Areas affected by poverty are the focus of ICTD, but any setting with limited connectivity, unreliable electricity supply and low literacy levels conspire to create a unique technological landscape that might be relevant to ICTD (Cobb *et al.*, 2018:1).

2.5 INFORMATION SECURITY

Ragaad (2010:5) emphasises that information security is now better understood by organisations because most of them have, in one way or another, experienced some harm produced by malware, intruders, or even their own employees. There is no single organisation that has not seen or experienced some undesired events that affected its computing environment and its information systems. Any one of the following experiences may have been inflicted on an organisation:

- theft, damage, or destruction of computer systems;
- corruption or destruction of corporate data;
- leakage of sensitive information to rivals;
- theft of private information for employees, customers or partners;
- damage to the reputation of an organisation; and/or
- denial of service that caused a business loss.

Intruders employ a variety of methods to conduct their malicious activities, and these are varied and often available for a fee or low cost on the internet, depending on their specifications.

According to Whitman and Mattord (2012:9), the following are key concepts within the information security space:

- **Access:** a subject's/object's ability to use, manipulate, modify or affect another subject or object.
- **Asset:** the organisational asset that is being protected.
- **Attack:** an intentional or unintentional act that can cause damage to or otherwise compromise information and/or systems that support it.
- **Control, safeguard or countermeasure:** security mechanisms, policies or procedures that can successfully counter attacks, reduce risk, resolve vulnerabilities and improve the security within an organisation.
- **Exploit:** a technique used to compromise a system.
- **Exposure:** a condition or state of being exposed.
- **Loss:** a single instance of an information asset suffering damage or unintended or unauthorised modification or disclosure.

- **Protection profile or security posture:** the entire set of controls and safeguards, including policy, education, training and awareness, and the technology, that the organisation implements (or fails to implement) in order to protect the asset.
- **Risk:** the probability that something unwanted will happen.
- **Subjects and objects:** a computer can either be the subject of an attack or an agent entity used to conduct the attack.
- **Threat:** a category of objects, persons, or other entities that presents a danger to an asset.
- **Threat agent:** the specific instance or a component of a threat.
- **Vulnerability:** a weakness or fault in the system or protection mechanism that opens it to attack or damage.

The need to protect organisational information security has been growing rapidly over the past decades due to the heavy reliance of modern organisations on their information systems. Organisations have realised that technological measures alone cannot protect the organisational information security; a significant number of end-users' efforts are required to perform information security behaviours.

This means that end-users play a critical role in reducing information system risks, but on the contrary, they are the weakest link in the information security chain (Dang-Pham *et al.*, 2017: 111).

Municipalities and NGOs are becoming aware that information security is an essential aspect of their business strategy, and as a result, they need to apply Information Security Risk Management (ISRM) to identify risk in the organisation and put measures in place to address these risks. There are a number of different types of risk management methods, standards and guidelines available to assess and manage the information risk aspect of an organisation (Shamala *et al.*, 2017:1).

Air traffic, defence, telecommunication, and water and electricity distributions systems are all examples of how dependent modern society is on information technology systems. For many years, ICT experts have focused on the technological aspects of information security to guarantee a secure environment for information.

It must, however, be acknowledged that the human aspects of information security play a vital role in this domain and should be taken into consideration along with the technological aspects (Safa *et al.*, 2017:1).

The role of insiders should always be considered to ensure that organisations can practice effective information security management. There are many users within the organisations that have the legitimate capability to access one or many systems through authenticated processes. An insider may not necessarily be required to spend as much effort and time in accessing the targeted information in comparison to external attackers.

The information contains key characteristics that make it desirable and valuable and this makes it even more valuable to the potential criminal. For instance, within a social engineering context, online or phishing scams require sensitive information for criminal purposes. The CIA triangle (confidentiality, integrity and availability) represents the three desirable traits of information (van Rensburg & Prinsloo, 2015:90).

Table 2.1 depicts the new security controls in terms of the **ISO** standards.

Table 2-1: ISO Standards Security Controls

New security control section	Description
A6.1.1	Information security in project management
14.2.1	Secure development policy
14.2.5	Secure system engineering principles
14.2.6	Secure development environment
14.2.8	System security testing
16.1.4	Assessment of and decision on information security events
17.2.1	Availability of information processing facilities

Source: Ukidve and Tadvalkar (2016:390)

In an effort to secure information, South Africa has tended to rely on security solutions from other countries. While this may seem like a desirable solution, safeguarding our national information and infrastructure using already-available technologies raises a number of questions. How well do we know or understand the technology that we are importing? How much permission are we given to control it? Clearly, blindly importing technologies to safeguard our critical infrastructure makes us very vulnerable (Nelwamondo, 2010:49).

2.6 SECURE TECHNOLOGY PLATFORMS AND CHANNELS

Thompson *et al.* (2017:376) acknowledge that the accessibility of the Internet has provided an immense social benefit by linking communities and dissolving geographic boundaries. Even though communities have been brought together by developments in technology, this free, borderless communication has opened up new avenues for crime and fraud which exposes millions of computer users to cybercriminals across the globe.

Security and privacy are critical features of current communication and information systems. Designing and implementing such features on a wide variety requires crossing the boundaries of multiple systems (PCs/laptops/smart-phones/tablets/network routers and many others) and these systems should be able to provide the ability of porting applications that include video, audio and data processing components (Ahmad *et al.*, 2013:1315).

As a result, systems designers (including security designers) are faced with different challenges in their quest to achieve portability and reusability, and top-down systems design still remains elusive features of the current system design practices.

According to Shanthi *et al.* (2018:1968), data storage in the cloud has become popular in recent times as the demand for outsourcing data has risen in order to assist organisations in managing their data. Therefore, the security and privacy of data can become a significant issue as data can be gathered from diverse clients and be hosted on virtual machines that provide a cloud computing environment for organisations.

Solomon *et al.* (2015:427) state that each and every organisation has a duty to understand which laws and regulations apply to them in order to employ necessary countermeasures to comply. Fiscal responsibility is the single most compelling reason to address security as the failure to secure an organisations' network exposes it to increased costs. Security breaches can be devastating to organisations to the extent that they never recover, thus making security a preservation and standard activity in the business world today.

Geier (2010:339) identifies the following elements as key for secure computing in an organisation:

- **Encryption:** scrambles the data frame to keep unauthorised people from seeing the actual information content of the frame.
- **Authentication:** ensures that client devices connecting to an access point are authorised to access protected resources.
- **Rogue access point detection:** the ability to detect and eliminate rogues that may be planted by hackers or even employees.
- **Radiofrequency (RF) shielding:** helps in minimising signal coverage from spilling outside of the controlled areas.
- **Security policies:** define security policies that best satisfy requirements and suit the environment.

Cloud computing has emerged as a prominent service paradigm of low-cost anytime and anywhere, computing for various business needs. Service providers of these cloud services need to ensure that their platforms are secured and as a result can offer the required dynamicity to the users and their workloads on the different services that they access through the cloud platform (Panneerselvam *et al.*, 2018:322).

2.7 SECURE SYSTEMS

Software-based systems are faced with security problems that may compromise their safety functions. Generally, security considerations have often been ignored in the system development process. To address this issue, security considerations in the development process of computer systems should be made as described in the industrial standards (Park et al., 2016:94).

In an ideal world, we would like to have computer systems that are entirely secure but past and current experiences have shown that even best attempts to build secure systems are not perfect.

Almasizadeh and Azgomi (2016:47) identified the following four main phases of insecurity in computer systems:

- **Design and development phases** – it would not be feasible to make computer systems' software and hardware components completely free of vulnerabilities.
- **Interaction environment** – the environment is very complex, and as a result, the behaviour of malicious attackers cannot be well understood.
- **Free available attacking tools** – conducting a large number of attacks against systems is a highly automated process.
- **Human-made errors** – errors that lead to security holes and flaws frequently occur.

Pervasive computing envisions a new generation of distributed systems where computers in their multitude are hidden in the background of the user and interact calmly to provide users with relevant information and services, anytime and anywhere. These computers will continuously gather and share any data about the users and their context that is relevant for their decision-making and also be able to adapt themselves to changing user situations while ensuring that disruptions are kept to a minimum.

Data that is transmitted may contain highly sensitive user information and to foster the widespread use of pervasive computing systems, it is critical to ensure that data that is exchanged, is securely stored in these systems. With the advances in technology, handheld devices are getting smarter by the day, store more user information and can

calculate the user's location at any time and communicate with the rest of the world via the Internet (Siewe, 2016:121).

Security attacks on electricity grids are also on the increase, and this can lead to considerable economic losses and increased environmental concerns. The security posture of the current electricity grids is inadequate to address all its existing and emerging security attacks. The concept and adoption of Energy Internet (EI) will significantly improve the security of the smart grid. EI is proposed as an integrated platform with multidirectional communication and power flow mechanisms designed for the improvement of the smart grid. The IoT technologies used to collect and analyse real-time data for intelligent energy management and with the EI ensures that energy domains, such as generation, transmission, distribution, operations, service provider, markets, end-users and regulators are seemingly integrated (Sani *et al.*, 2018:1).

The IoT allows devices to be connected wirelessly so we can interact with them anytime, anywhere. IoT introduces new innovative features to devices that have been around for decades and while connecting all these devices makes our lives easier, adding connectivity brings a whole new set of challenges to system design and security (Gupta & Dham, 2017:16).

The protection of sensitive data represents an urgent need for secure communications, especially with innovation and modern ICT, such as fog-cloud IoT. Fog-cloud IoT is a new paradigm and an incredible technology for equipping quickly deployable and scalable information technology solutions at conservative network bandwidth, reduced infrastructure costs, low latency, location awareness and mobility support.

Fog-cloud IoT is a trusted and dependable solution to bring the services and resources of the cloud closer to users and thus assist in leveraging the available services and resources on the network. However, fog-cloud IoT services lead to privacy and security issues and challenges as any transmission of data through unsecured and open channels, such as fog-cloud IoT, is an issue that security designers should address (El-Latif *et al.*, 2017:10332). The aforementioned will also ensure that the problems of illegal connections and purchases of electricity can be minimised both in the interest of the users and the service providers.

The capabilities of the systems have contributed to efficiency increases, as well as opening new types of business and social activities. Personal banking, communications and expectations have shifted in how people conduct business or stay in contact with each other.

Secure systems should support globalisation and rapid business change through the sharing of information, shifting of jobs, and the creation of new jobs and whole new career types (Morley, 2010:235).

The growth of wireless network devices in medical services has gained an inevitable pace to offer various applications in healthcare. Telecare Medical Information Systems (TMIS), like all the other systems, have their own security concerns and issues that need to be addressed. Medical information should be protected through authenticated channels and cryptographic solutions. Although there are still concerns around the level of security required for telemedicine applications, however, to date, it is still a challenge to provide an efficient and secure system which will be able to address all the requirements of secured remote medical services (Rezaeibagha & Mu, 2018:24).

According to Maglaras *et al.* (2018:42) Industrial Control Systems (ICS) have become a critical component within process automation technologies, such as Supervisory Control and Data Acquisition (SCADA) systems and Distributed Control Systems (DCS), which have been subject to a growing number of attacks in recent years. As these systems deliver vital services to critical infrastructures, such as communication, manufacturing and energy amongst others, hostile intruders mounting attacks represent a severe threat to the day-to-day running of organisations.

ICS generally have unique performance and reliability requirements and often use operating systems, applications and procedures that can be considered unconventional by contemporary IT professionals. These requirements typically follow the priority of availability, integrity, and confidentiality together with the management of processes that, if not correctly executed, can pose a significant risk to the health and safety of human lives, damage to the environment, as well as serious financial losses.

2.8 CYBER SECURITY

According to Yasin *et al.* (2018:179), the most crucial prerequisite for successful system development is understanding the security requirements of an organisation. Many researchers have a burning desire to make security requirement activities more engaging, enjoyable, and rewarding in order to improve security requirement training/awareness and therefore increase its impact on the organisation. Stakeholders play an important role in the requirement elicitation process, their presence and contribution improve the quality of requirements and ultimately have a positive impact on the system to be developed and the security thereof.

Humans are often identified as the weakest link in cybersecurity since any technical security solution is still prone to failures caused by human errors. As such, there is a considerable amount of research that seeks to better understand users and the factors that influence their behaviour towards cybersecurity. Understanding how users' individual differences influence their cybersecurity behaviour intentions is critical in helping researchers, security practitioners, and organisations to identify users who are more susceptible to poor or potentially dangerous security practices (Gratian *et al.*, 2018:345).

More and more citizens are making use of the Internet (email and worldwide web), and this increased use can lead to many violations of security by criminals, which is commonly referred to as cyber security. As the focus shifts increasingly to the need to improve security in cyber-space there are two critical areas of focus that needs to be addressed: the nature of the hazards and the required countermeasures; and users' engagement with the cyber-space and their perceptions of risk (van Schaik *et al.*, 2017:547).

According to van Solms (2015:44), cybercrime is growing at an alarming rate in Africa, more than in other continents, and according to the Microsoft Report of 2011, malware infections in Africa are higher than the global average. This is due to the fact that more people in the African continent are utilising technology and cybercriminals are developing their strategies to exploit cybersecurity gaps as well as users trusting nature towards technology.

Egelman and Peer (2015:16) argue that several researchers have identified differences in human traits that correlate with poor security practices and increased susceptibility to becoming a victim of cybercrimes such as phishing or social engineering but work in this area is relatively limited at this stage.

Vicious attacks and threats occur at any time and anywhere in cyberspace. Security experts have developed automated defence measures have been developed to protect organisations' critical information infrastructure, such as Intrusion Detection Systems (IDS), firewalls, anti-virus software, vulnerability scanning tools, and Security Information and Event Management (SIEM). Many organisations have built Security Operations Centres (SOC) to provide central control of the network monitoring and defending issues (Zhong *et al.*, 2018:12).

The challenge with SOC operations is that they are a heavily human-in-the-loop process: given the data collected by the cyber defence measures (IDS alerts & firewall/SIEM reports)/ Cyber-defence analysts need to make sense of the data to achieve cyber situational awareness in order to enable the incident response team to take timely and effective actions against threats. Three questions need to be investigated to gain cyber awareness:

- Is the network currently under an attack?
- How did the attack happen?
- What will the attackers do in the following steps?

These questions are critical in providing answers to the necessary foundations that need to be laid out in the complex cyber-world environment.

A close evaluation of cyber-criminal activities reveals numerous areas of concern including cyber vandalism (defacement), hacking, denial of service (DoS), domain name hijackings and dissemination of viruses. The most common forms of cyber-attacks include DoS, website hacking, malicious software (malware), phishing and spam emails (Alali *et al.*, 2018:325).

2.9 ICT POLICIES

In recognition of the importance of ICT Governance, a number of internationally recognised frameworks and standards, have been developed to provide context for the institutionalisation of the governance of ICT.

- **The King III Code:** The most commonly accepted corporate governance framework in South Africa is also valid for municipalities. ICT was used to inform the governance of ICT principles and practices and to establish the relationship between corporate governance of and governance of ICT.
- **ISO/IEC 38500:** Internationally accepted as the standard for corporate governance of ICT; ICT provides governance principles and a model for the effective, efficient, and acceptable use of ICT within municipalities.
- Other internationally accepted process frameworks for implementing Governance of ICT (Municipal Governance of ICT).

ICT has brought about revolutionary changes in the way people work, communicate, learn, spend time and interact. ICT has also profoundly transformed business and government practices. The impact of the ICT revolution is now palpable in all countries and are projected to be economically and socially revolutionary in the coming years as technology penetrates and fosters fundamental change in all sectors and dimensions of life (Jorgenson & Vu, 2016:383).

Users who procrastinate or in the worst cases, intentionally resist change poses a severe threat to their organisations while those who conform and adopt new policies early, present several benefits to their organisations. Early conformers are less costly to support than late or no-conformers who create last-minute rushes to security changes that may crash the system, overload the help desk, or cause hotline traffic jams. A lot can be learned by focusing on users who are not only compliant but also conform to policy requirements early in the process (Belanger *et al.*, 2017:887).

One of the key pillars and operational priorities in developing countries is to support local firms and small and medium-sized enterprises (SMEs) in order to open the market for foreign investments into such countries. A vital feature of this is the ability to use

technology and find innovative ways to enable such technology. Innovation in the ICT space has its own challenges.

Policies are required to support technology and innovation development so that the efforts of research and development (R&D) in organisations can lead to effective technology commercialisation, bringing about business creation and economic growth. This simply means that government needs to play an active role in providing funding mechanisms that support organisations, nurture the development of technology and assist in the process of commercialising innovations in the ICT space (Wonglimpiyarat, 2014:467).

(Buys, 2000:33) encourages organisations to implement Electronic Communications Policy (ECP) that deals with, amongst other things, acceptable e-mail and internet use, representing the firm in an e-mail message and computer security. Employees should not be allowed to use unchecked diskettes, download data from the internet without authorisation or open e-mails with strange (yet inviting) attachments.

Oxley (2013:144) argues that with the increase in users who participates in the social networking platforms, ICT policies that govern security controls should be in place to address the following:

- all matters relating to social network security;
- determine which employees should have access to social media sites;
- decide which social media sites should be prohibited;
- decide which mobile devices will be allowed to access social media sites;
- assign staff to update social media content and respond to messages;
- allocate a role for reviewing the tactics for using social media and their alignment to departments' policies and strategy; and
- decide what content needs to be curated.

Bauer *et al.* (2017:146) explain that besides technology, the biggest threat for Information Security (IS) is human behaviour. Users regularly cause IS incidents by volitional or non-volitional risk-taking behaviour, such as careless information handling, surfing on unsecured webpages, thoughtless usage of mobile devices, or non-secure data practices. It is important for many organisations to implement preventive controls such as Information Security Policies (ISP) to introduce a binding standard concerning IS behaviours amongst all users in an attempt to reduce/minimise IS-related loss incidents.

These ISP policies should outline specific security requirements, but they cannot work alone and requires organisations to concentrate on continuous employee Information Security Awareness (ISA) which is often described as ‘a state where users in an organisation are aware of their security mission’.

2.10 CONCLUSION

Chapter 2 reviewed literature on the subject of a secure computerised environment and the different elements that can contribute to such an environment.

The chapter begins with an introduction on what is referred to as a secured computerised environment. In the overview part of the chapter, context is provided on the different platforms that are available to users and their potential threats and also the recent developments in the US and Europe, respectively. The potential impact of the social media space in the context of government protests is reviewed, as well as what the Johannesburg Metropolitan Council has implemented in partnership with FNB.

The impact of cybersecurity is also considered in relation to the developing countries, such as South Africa, Zimbabwe and Nigeria with their increased level of internet users. The remainder of the chapter looks at each of the elements that make up a secure computerised environment. Details are provided in terms of how each of these elements can contribute towards a secured platform as well as the challenges that they can bring into any organisations if not adequately managed or addressed.

The chapter concludes by looking at what system designers need to look out for in their quest to improve the security of their systems. The most forms of attacks are identified, and I conclude by looking at cloud computing and how it has contributed to providing users and service providers with the assurance of a secure platform.

The next chapter in our research study presents the different research paradigms, research methodologies, population and sample of our participants as well the data collection method used in our research study.

CHAPTER 3: RESEARCH DESIGN AND METHODOLOGIES

3.1 INTRODUCTION

This chapter looks at the research design and methodologies that can be used in the study and how it provides guidance in addressing the primary objective of providing a managerial framework for a secure computerised environment in a metropolitan municipality.

The chapter starts with a discussion of the different research paradigms that exist, their role, where they originate and their principles and position in the research space. Research design and methodology are subsequently discussed.

The different research design methods, the population and the different sampling methods are explained. The chapter is completed by probing the data collection method to be used and the different techniques that can be used for collecting data from the participants.

3.2 DIFFERENT RESEARCH PARADIGMS

(van Zyl, 2015:2) argues that a paradigm is regarded as a world view or a general perspective, a way of breaking down the complexity of the real world. As such, paradigms are embedded in the socialisation of adherents and practitioners: paradigms tell them what is necessary, legitimate, and reasonable. Paradigms are also normative, telling the practitioner what to do without the necessity of long existential consideration.

It is, therefore, that particular aspect of the paradigms that constitutes both their strength and their weakness – their strength in that it makes action possible, while their weakness in that the very reason for action is hidden in the unquestioned assumptions of the paradigm.

According to van Zyl (2015:2), a fervent debate has been going on about quantitative and qualitative research paradigms since the last part of the 19th century. Quantitative purists have expressed assumptions that are consistent with a positivist philosophy, whereas qualitative purists (i.e. post-positivist, post-structuralists, and post-modernists) reject positivism.

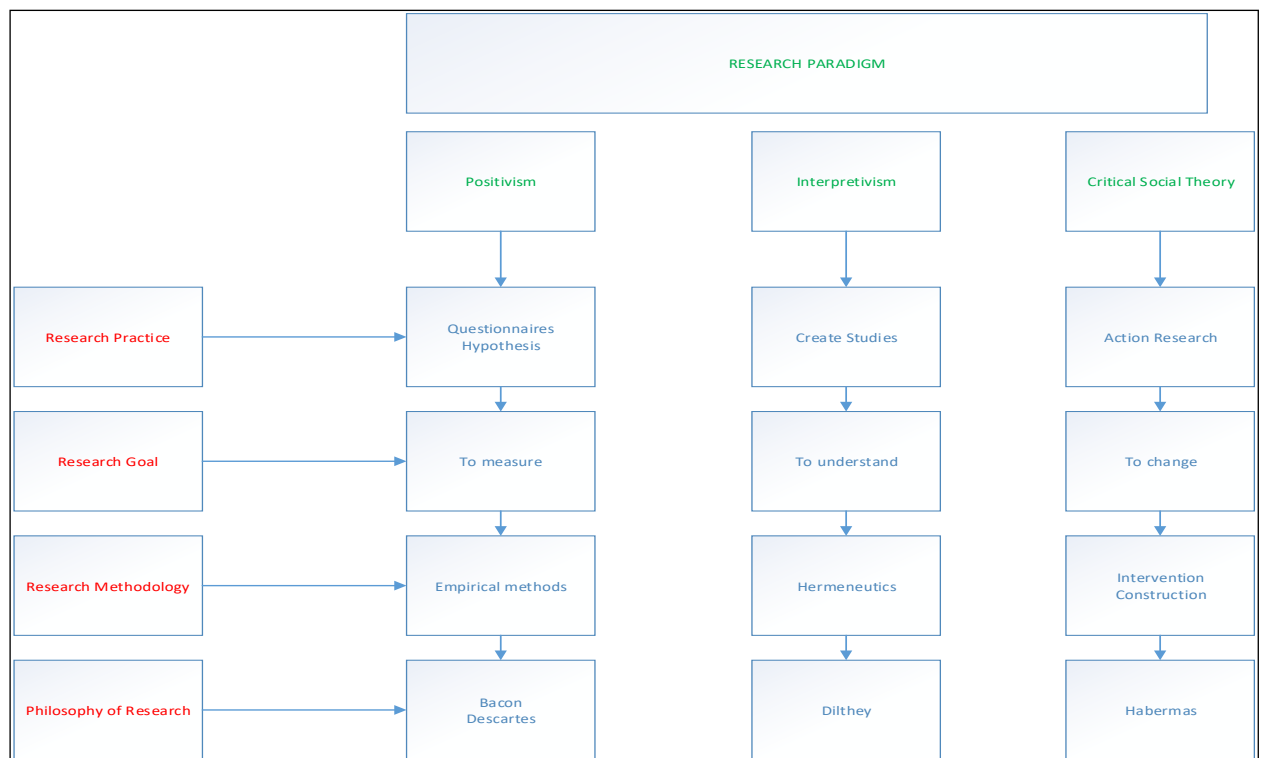


Figure 3-1: Different research paradigms

(Source: Chilisa & Kawulch, 2012:53)

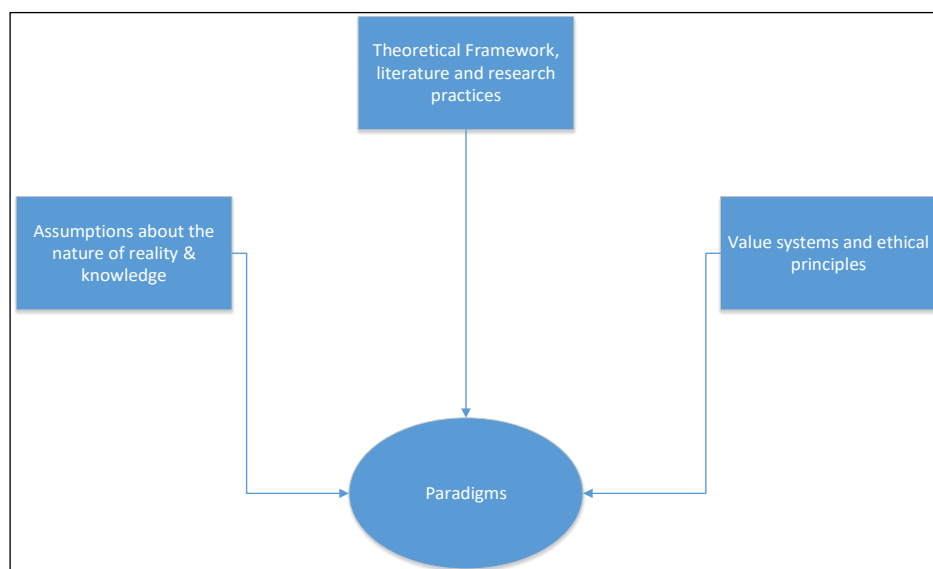


Figure 3-2: Factors affecting the choice of a Research Paradigm

The significant differences that exist between the two sets of purists are at the level of the logic of justification. Unfortunately, much of the quantitative-qualitative debate has involved the practice of polemics, which has only caused further confusion rather than to clarify and to divide as compared to unite educational researchers (Onwuegbuzie, 2002:518).

3.2.1 Positivism

According to Bertucio (2017:479), Descartes must be credited to some degree for ushering in an epoch of scientific advancement and its increased attention in material comfort and human longevity. It is also impossible to speak of Descartes' method without noting his foundational contribution to modern science as well as how he had always seemed to desire a path to knowledge that cannot be derailed by human fallibility.

Positivism emerged as a philosophical paradigm in the 19th century with Auguste Comte's rejection of metaphysics and his assertions that only scientific knowledge can reveal the truth about reality. It was later formally established as the dominant scientific method in the early parts of the 20th century by members of the Vienna Circle.

The Vienna Circle sought to construct a unified scientific world-conception that rejects the use of philosophy as a means of learning about the true nature of reality. Unfortunately, it failed as a coherent philosophy of science because of the many inconsistencies between its theory of reality and its theory of knowledge (Kaboub, 2008:343).

During the 1960s, neo-Marxism managed to infiltrate the mindscape of young intellectuals both in Europe and the US , and in doing so it played a decisive role in the revolutionary events of the late 1960s (student revolts).

In Paris, France, students advanced with banners claiming that the idea of an objective and neutral science was suspect. They viewed social theory by definition to entail social critique, i.e. if one cannot envisage society to be different from what it is, then the researcher is enslaved merely to follow its footsteps uncritically (Strauss, 2003:257).

According to Scharff (2007:511), it is difficult not to hear premodern accounts of philosophical inquiry as strangely indirect and unsatisfactory to the modern ear. Researchers and scholars have learned that the mind must be methodologically prepared for thinking. It must be rule-governed, deliberate, at least to some extent distrustful of its very willingness to seek the truth. Genuine thinking only begins when the mind follows something like an 'order of reason', after first withdrawing allegiance from the pre-existing and ill-acquired beliefs that constitute our initial condition.

Philosophers as different from each other as Descartes and Hume have thought it possible for an individual mind to classify and recognise its own thoughts and experiences while holding in suspense the question of the existence of the external world and of other minds. And as a result, such a supposition seems to entail the possibility of a private language or of something very like one (McDougall, 2017:553).

Hassan and Mingers (2018:569) focus on the work Bacon which refers to as the scope of philosophy of science that addresses not only the goals of research but also whether such research qualifies as being scientific, as it deals with what science is, how it works and the justifications through which we build our knowledge.

During the first decade of the 21st century, neopositivist claims made about the nature and validity of knowledge in the debates about scientifically-based research was countered by educators who, decades earlier, had made various turns away from positivism and were surprised by its resurgence. In those debates, positivists often used postmodernism as a code for any social science approach that was not positivist and so, they claimed, could not be scientific (St. Pierre, 2012:483).

3.2.2 Interpretivism

According to Chowdhury (2014:433) interpretivism refers to the approaches which emphasise the meaningful nature of people's character and participation in both social and cultural life. This approach denotes that the methods of research which adopt the position that people's knowledge of reality is a social construction by human actors, and so it distinctively rules out the methods of natural science.

Interpretivism has its roots in the philosophical traditions of hermeneutics and phenomenology, and the German sociologist Max Weber is generally credited with being the central influence of this approach.

Interpretive research and its closely-related cousin, qualitative research, have achieved some degree of acceptance in the academic discipline of IS. Accompanying the price of acceptance, however, has been some loss of clarity in what makes interpretive research different, special and valuable when compared to positivist research.

A result of this is a position, recently advanced, that positivist research and interpretive research are essentially the same. One may, of course, define them so that in effect, they are the same. However, the original attraction of interpretive research for the positivist mainstream was the formers' promise of insights not readily accessible to the latter (Hovorka & Lee, 2010:2).

Interpretivists such as Dilthey, maintain that interpretivism is not just a desirable mode of analysing politics, and interpretation is not avoidable since the establishment of knowledge depends on it. Knowledge, interpretivists insist, is generated as we interpret new experiences or new theories in the context of what we believe and what we have learned (Hall, 2014:308).

3.2.3 Critical Social Theory

Social research is underpinned by the background knowledge of the social relationships that give importance to the topic and the possible results of our scientific activity. Although this may be true of research altogether, researchers need to build critical social research on this insight. However, since critical social research is supposed to be related to social reality as it not yet is, one always has to theorise a teleological conception of the social world (De Angelis, 2015:172).

According to Kirkpatrick (2003:92), Habermas counsels us to be cautious in the use of evolutionary concepts and categories. He is not interested in developing an overarching 'super historical theory' that can account for all epochal transitions. He assumes the existence of an evolutionary logic at work in specific key dimensions of society that may prove fruitful for sociologists seeking to identify the development process that explains actual social changes.

Hadfield (2012:572) reflects on the critique of those who attempted to link critical social theory and action research in that it operates at two levels. First, at the level of the general cultural and the critical discourses that surround action research, and that the introduction of such theories has been practically 'disabling' rather than enabling. The typology of action research, which identifies technical, practical and emancipatory forms, are used as examples of how this discourse has selectively undermined the value of certain forms of action research while simultaneously promoting the significance of action research's more critical forms.

On design science, Gantt *et al.* (2016:132) mention that few scientists today would claim that (certainty) is ever entirely possible. They accept that since human perception and understanding are fallible, people will always be somewhat selective and biased by their preconceptions. However, most scientists (including experimental social psychologists) take the position that by using the scientific method they can progressively pin down 'the facts' and get close enough to reality to develop working models of how processes and phenomena 'work' in systematic, lawful ways.

The positivist approach has been chosen for these research study. This approach that has a philosophy from writers such as Bacon and Descartes which is founded on the research practices of Hypothesis and Questionnaires. The approach also supports Empirical method in the research methodologies and the ultimate goal of the positivism approach is to measure, all these are key areas that are applicable to our research study.

3.3 RESEARCH DESIGN AND METHODOLOGY

Researchers typically ask two fundamental types of questions: (i) What is going on? and (ii) Why is it going on? To answer the first question (What is going on?), the researcher needs to examine the various philosophies, the use of literature in research and in the design techniques, integration of theory in research, and developing the theoretical perspective of research. The second question is answered through the framing of research questions under the qualitative, quantitative and mixed methods approaches and the illustration of how the various research designs are able to answer the primary research questions (Gurtoo, 2011:683).

Qualitative and quantitative researchers alike struggle to represent their findings in complete ways. Even quantitative research, often favoured as scientifically based, straightforward, and objective, involves a series of subjective decisions. Qualitative research, at its best, generates multiple, frequently conflicting perspectives and accounts (Holley & Colyar, 2012:114).

The focus of research is generally words, texts and images as opposed to gathering of statistical data (numbers) and using language focused on variables, with the goal of generalising and confirming research hypothesis. However, these differing emphases do not mean that qualitative researchers do not use numbers or that quantitative researchers do not use words (Hesse-Biber, 2016:6).

According to Punch (2014:114), the three uses of research design can be distinguished in the literature, ordered from general to specific.

- **Most general level** – it means all the issues involved in planning and executing a research project, from identifying the problem through to reporting and publishing the results.
- **Most specific level** – refers to the way a researcher guards against, and tries to rule out, alternative interpretations of the results.
- **Between the two (specific and general)** – situating the researcher in the empirical world and connecting research questions to data.

Researchers may follow traditional processes to define the focus of the research, including examining the existing literature to identify possible topics and research questions that may contribute to their research objectives/goals. In practice, of course, gaining clarity about research questions often occurs through an iterative process of data gathering and continually returning to the literature. This approach is true of quantitative studies as well as qualitative and mixed-methods investigations, regardless of how simplistically the research process is rendered in published accounts (Fassinger & Morrow, 2013:73).

3.3.1 Qualitative research

A qualitative researcher guided by a research question acts as an instrument, since the line of questioning may change during data collection as new understanding is gained and/or the situation changes. The data from research is derived from observation, interviews or verbal interactions, focus group discussions, document reviews, life histories, etc., and the researcher asks why, how and under what circumstances things occur; and not just what, when and where (Tarin, 2017:5).

A lot of qualitative studies describe the diversity of certain cognitions or behaviours in a population by means of semi-structured interviews with a small sample of population members. This type of qualitative research remains undefined in the methodological literature. However, it is argued that most of these studies may well be typified by the label, 'qualitative survey'. While the statistical survey analyses frequencies in member characteristics in a population, the qualitative survey analyses the diversity of member characteristics in a population (Jansen, 2010:1).

Schurink (2009:805) argues that a qualitative design, if properly designed, could be used as a tool to unlock the empirical world. It provides the researcher with the markers, parameters and tools to proceed.

The following are the fundamental elements of qualitative research design:

- the research approach guiding the study;
- the research question to be answered;
- the research strategy or reasoning to be implemented;
- the research setting to be studied; and
- the methods to be used to gather and analyse data.

The impact of new technology both on what kinds of data can be collected and recorded and on what kinds of analysis it makes possible has continued to the present day. In the 21st century, the use of new technology still raises issues like what should be analysed, how it should be analysed and in what ways the knowledge and understanding gained are different and more/less well-founded than those gained in more traditional ways. The majority of researchers are aware that new ways of recording and collecting data, and new ways of undertaking analysis are affected by technology (Ribbs *et al.*, 2002).

Qualitative research and formal modelling are often regarded as mutually exclusive. Qualitative methods provide rich and detailed descriptions of social phenomena based on propositional rather than numerical data and can account for the meanings actors themselves give to their behaviours and attitudes. However, context-dependence and unrepresentative sample formation hinder the generalisation of results. In contrast, models provide simplified, abstract representation of reality, uncovering the underlying structure of a phenomenon and potentially deriving universal conclusions (Tubaro & Casilli, 2010:60).

Arora (2017:196) explains that proper qualitative research should have a clear purpose marked by predefined approaches to work upon data that is generated during the course of the study. In carrying out rich qualitative research, the following steps must be followed:

- understand the broad research question;
- exploration of literature focusing on the context of study;
- eliciting human experiences;
- continuous data collection and churning; and
- interpretation of data and conclusion through evidence.

3.3.2 Quantitative research

The research argument can be summarised as that the integration of a quantitative approach is necessary to adequately tackle central research questions, and ensure that the information obtained from the qualitative research is indispensable to enable the researcher to determine reasons for any errors that may occur and the impact that they may have on the overall research (Horvath, 2012:1748).

Quantitative research is typically associated with a positivist and objective stance, while qualitative research is associated with an interpretive and constructive one. However, the often stark contrasts that are sometimes drawn up in accounts of the differences between quantitative and qualitative research, possibly exaggerate the differences between them (Alasuutari et al., 2009:13).

According to Lach (2014:88), quantitative research with data collected through the numerical measurement of specific phenomena and analysed during mathematically-based methods (particularly statistics), is common to both natural and social scientists.

Researchers are trained in multiple ways to reduce bias, including operationalisation of questions, sample strategies, research design, control groups, and robust statistical techniques, each with their own requirements of data collection.

Quantitative research methods are procedures and techniques used to analyse data numerically, they include a study of the valid methods used for collecting data in the first place, as well as a discussion of the limits of validity of any given procedure, (i.e. an understanding of the situations when a given procedure yields valid results), and of the ways the results are to be interpreted (Antonius, 2013:4).

Bader (2014:535) challenges and strongly critiques much that is taken as gospel in the quantitative methods approach, the use of which often results in misleading research. He sees the need for both quantitative and qualitative research, with the latter able to give more recognition to political, institutional and social dimensions and better suited to deriving meaning from research results.

One of the characteristics associated with students in a quantitative research methods approach is their anxiety, particularly their math or statistics anxiety. Math anxiety is defined as 'a euphemism for debilitating test stress, low self-confidence, fear of failure, and negative attitudes toward mathematics learning' (Lin *et al.*, 2016:392).

3.3.3 Mixed methods

While population scientists historically have relied primarily on surveys and censuses, there has been a recent shift towards mixed-method research, which can contextualise and validate quantitative analyses. In mixed-methods research, the strengths of one method can make up for the weakness of another, and as a result, there has been a significant increase in the significant population studies journals reporting on mixed-methods research (Schatz & Williams, 2012).

It provides a researcher with a combination of controls of both extraneous variables and reduction of error variance through triangulation or seeking convergence of results. The option exists to convert quantitative data into qualitative or vice versa for comparison, and a story is formulated to explain the phenomena studied and it can be generalised (Kiessling & Harvey, 2005:31).

According to Steen *et al.* (2018:11), the debate about whether and how qualitative and quantitative research methods should be combined in social sciences is not new, although it has gained importance over the past ten years. With mixed methods research designs, researchers usually refer to the combination of qualitative and quantitative data analyses (rather than a mix of different quantitative or qualitative methods).

From a view of primarily qualitative research approaches, this view is not entirely new at all and is often referred to as data triangulation, contributing to higher levels of reliability and substantiation of the construct.

Mixing the research methods has become a commonplace amongst researchers, such that the rationales, goals, and means for evaluating research are continuously being combined. This shifting and blending have made it difficult to distinguish between research approaches, raising the question of whether there are, in fact, any meaningful differences between the different research approaches (Walsh & Koelsch, 2012:380).

Observation as a research method is highly flexible and covers a spectrum of activity. In qualitative research, observation is likely to be linked with ethnography but it is often used in case studies and sometimes in grounded theory. The observation of what people do and how they do it can lead to revealing and compelling data.

There are concerns, however, that observation as a research method is potentially complex and can be daunting to novice researchers because of practical and ethical concerns, including how to record the data so that it is an accurate representation. Other researchers may challenge observation research on the credibility of its data, on whether or not people observed will change their behaviour, and whether or not the data collected represents what happened (Baillie, 2013:4).

Mixed-methods research capitalises on the strengths of both qualitative and quantitative methodologies by combining approaches in a single research study to increase the breadth and depth of understanding. This type of research method can be a better approach to research than either quantitative-only or qualitative-only methods when a single data source is not sufficient to understand the topic when results need additional explanation, exploratory findings, need to be generalised or when the complexity of research objectives are best addressed with multiple phases or types of data (Wisdom *et al.*, 2012:722).

3.4 POPULATION AND SAMPLE

3.4.1 Population

The research population in this study comprises of male and female employees in the ICT departments of the following entities within the CoJ metropolitan municipalities:

- Johannesburg City Power
- Johannesburg Water
- Pikitup
- Johannesburg Roads Agency
- Johannesburg Fresh Produce Markets
- Johannesburg City Parks and Zoo
- Johannesburg Metrobus
- Johannesburg Metro Trading Company
- Johannesburg Theatre
- Emergency Management Services
- Johannesburg Development Agency
- Johannesburg Property Company
- Johannesburg Social Housing Company

3.4.2 Sample and sampling method

There are a number of requirements for a sample. The sample should be a minimised representation of the population in terms of the heterogeneity of the elements and the representatives of the variables. The elements of the sample have to be defined, with the population clear and empirically defined to ensure that there is a clear limitation on the population (Flick, 2011:71).

Uprichard (2013:1) explains that sample design is a well-recognised issue in social research and as any research methods textbook will try to convey, the internal, as well as the external validity of any empirical study, rests to a large extent on the adequacy of the sample to be able to meet the research aims and objectives.

According to Elliot *et al.* (2009:56), researchers and scholars should consider the situations in which externally observable characteristics allow experts to quickly categorise participants as likely or unlikely to contain a member of a rare target population.

This classification can form the basis of disproportionate stratified sampling such that participants classified as unlikely are sampled at a lower rate than those classified as likely, thereby reducing screening costs. The design weights account for this approach and allow unbiased estimates for the target population.

When a sample is to be drawn from a population, it is necessary to be able to construct a sample frame that lists suitable sample units that encompass all elements of population. If it is not possible or feasible for all of the elements of the population to be listed, some clusters of elements can be used as sampling units (Raina, 2014:149).

Miller *et al.* (2010: 438) state that purposive sampling that seeks to draw from a broad cross-section of users and to sample a relatively large number of individuals, can give rise to samples of a population and may be considered sufficiently representative to reasonably warrant the drawing of inferences relating to the entire population.

Commonly used sampling methods for the identification of participants in a particular population group vary from random to purposive. It might be expected that researchers should randomly sample from among eligible individuals in a population group, but this approach is resource-intensive and less demanding sampling methods have performed well in eliciting information that reflects broadly held ideas and views by the population group (Valero *et al.*, 2016:2).

3.4.2.1 Probability sampling

Smith *et al.* (2011:122) explain that probabilistic survey design principles have been successfully applied for decades in a variety of disciplines including agriculture, human health and natural resources. These statistical techniques have the advantage of generating population-level metrics, as well as optimising sampling efficiency to obtain high precision estimates at low sample sizes. According to Rahi (2017:3), probability sampling is a sampling approach in which each unit has an equal chance of probability to be selected. Probability sampling is further divided into the following five categories:

- **Simple random sampling:** is a sampling process in which each unit of the population has an equal probability of inclusion in the sample.
- **Systematic random sampling:** probability sampling technique where the initial sampling point is selected at random and then the cases are selected at regular intervals.
- **Stratified random sampling:** a process of sampling in which each subgroup called strata is given an equal chance to be selected randomly.
- **Cluster sampling:** a technique where the researcher derives a sample out of aggregations of the population that are geographically dispersed and possibly unable to access at the same time.
- **Multi-stage sampling:** involves a sequence of stages.

3.4.2.2 Non-probability sampling

Aoto *et al.* (2014:31) explain non-probability sampling as a recognised and powerful tool that affords significant time-savings in the acquisition of data by sampling only a percentage of the overall sample size.

Rahi (2017:3) defines the following non-probability sample methods:

- **Convenience sampling:** a process of data collection from the population that is close at hand and easily accessible to the researcher.
- **Snowball sampling:** researcher makes initial contact with a small group of people who are relevant to the research topic and then uses them as referrals to make contact with others.
- **Quota sampling:** defines the strata of the population and sets a quota for the sample element of each stratum.
- **Judgement sampling:** a process where the researcher uses own judgement to select a group of people who knows about the problem.

A sampling technique used for a specific study may result in final scores that are low on external validity, and therefore making a conclusion based on non-probability (e.g. convenience sampling) not to be correct (Meenakshi *et al.*, 2015:487).

According to Dutwin and Buskirk (2017:213), non-probability samples have gained mass popularity and use in many research circles, including market research and some political research. One justification for the use of non-probability samples is that low response rate probability surveys have nothing significant to offer in a research process.

Laher, 2016:320) states that the assumption that 'bigger is better' applies most to the quantitative tradition in that this type of research seeks to generalise and predict, and as such it can only do this if samples are large enough and from representative groups. Unfortunately, there is no simple rule or guideline as to how large a sample should be.

3.5 DATA COLLECTION METHODS

One of the most far-reaching decisions a researcher must make is the way in which data will be collected. Should an interviewer ask the questions and record the answers, or should the survey be self-administered?

If an interviewer is to be used, there is a further decision about whether the interview will take place in person or over the telephone. If the respondent is to read and answer questions without an interviewer, there are choices about how to present the questionnaire to the respondents (Fowler, 2014:69).

According to Etchegaray and Fischer (2011:144), researchers should undertake a bit of pre-testing in the survey process prior to administering the actual (final) survey to the participants. Although the specifics of pretesting may vary amongst researchers, the primary goal should remain the same: to make sure that the survey items can measure the domains of interest reliability and validity when used in real situations.

3.5.1 Questionnaires

Research surveys have traditionally used paper and pencil self-administered questionnaires to collect information. However, with the growth of internet use, web-based questionnaires have become an important alternative to paper and pencil. Mixing both these data collection methods in one survey can lead to mode effects by simultaneously creating selection and measurement effects (Braekman *et al.*, 2018:2).

Issues of concern should be the content and construct of validity, single versus multiple-item scales, reversed item practices, response style effects, the number of scale points and scale polarity, numbering and labelling. The above guidelines should allow researchers to optimise study designs and to carry them out in the correct way (Geuens & De Pelsmacker, 2017:84). Researchers need to ensure a suitable composition and measurement sequence for an experimental questionnaire and to extensively discuss issues such as the briefing of participants, dichotomising, replication factors and robustness checks, and quality control measures.

Researchers can conduct interviews using immediate retrospective probing. This method involves participants completing the questionnaire one page at a time, with a cognitive interview conducted at the end of each page. The primary purpose of the cognitive interviews is to improve the item quality of the questionnaires, by uncovering the cognitive process that the participants use to answer the question items (Murphy *et al.*, 2018:3).

3.5.2 Interviews

Interviewing is, by definition a two-way exchange in which questions are asked and answered, the experience shared, attitudes outlined and perspectives on particular topics set out and explained. All sorts of methodological principles and values are then applied to this, but the expectation in qualitative interviewing is that two or three people will participate in a spoken discourse which is reciprocal and reasonably balanced between talking and listening (Keightly *et al.*, 2011:508).

Walking interviews are a method used by many researchers inside and outside of academia. Walking interviews provide researchers with the potential to bolster and add new layers of understanding to social science research. Over the past few years, researchers have made use of audio and video recordings to conduct their interviews. There is no need for any heavy equipment to be used, it is now possible to record interviews with most mobile phones, and other mobile recording equipment is affordable and widely available (Parent, 2016:523).

According to McCarthy (2016:37), the value of qualitative, face-to-face interview methods can be beneficial to the researchers. Participants of these interviews need to be approached sensitively, as the interview engagement demands a particular awareness of ethical issues, participants' choice and peer concerns, but once all of these factors have been addressed, rich data can result.

Dowling *et al.* (2016:679) argue that while interviews remain the mainstay of qualitative methods, they do not do so in isolation, being used as a supplement or to complement the other means of approaching, analysing and intervening in social life. This enriching of the interview includes the digitalisation of social life, as well as an increasingly prevalent concern of approaching life 'on the move' or as it happens. Enrichment also occurs through ongoing critical reflection across the different theoretical traditions of qualitative geographic research.

Criticism against the interview process as part of the research is that identity is formed through the creation of an alternative other. For a lot of researchers, the world is structured around binaries: foreign countries constitute the domestic, the outsider the insider, the man the woman, the third world and the first world, and the stranger constitutes the familiar self.

Given this dynamic, interviews and fieldwork in general might provide a profound challenge to the researchers' sense of themselves, as well as their understanding of the world (Gallagher, 2016:445).

3.5.2.1 Structured interviews

Swider *et al.* (2016:627) state that structured interviews produce overwhelming, more accurate and reliable ratings of research content than unstructured interviews. Numerous possibilities may explain why information transmitted during rapport building affects the quality of the information provided during the standardised question and answer portion of the interview.

When a researcher makes use of structured interviews, the sequence of the questions is important to minimise the potential impact of context effects. A key benefit to the structured interview is that the data can be collected by an inexperienced interviewer in a rote, formulaic manner (Cornell *et al.* 2013:137). According to Hartwell *et al.* (2016:757), a lot of research has been conducted around the interviews, including factors pertaining to the interview itself, the characteristics of the participants and the interpretation of the data collected from the structured interview.

A researcher needs to ensure that they are well prepared for conducting the interview with a view of obtaining as much relevant information as possible from the interviewee within the agreed time of the interview. The most significant benefit of the structured interview is that it expands on the traditional interview and address context specificity. Traditional interviews typically aim to assess professionalism and interpersonal skills, however, structure interviews as such that all participants in the research process respond to the same scenarios and questions, and allow for flexibility in what is asked at a specific point and generally requires fewer resources (van der Spuy *et al.*, 2016:180).

Researchers must find methods of capturing data that is consistent, cost-effective, and user-friendly to allow analysis and meaningful use of the collected data. Optimally, the capturing of data should require minimal manual effort and not be intrusive to their typical daily work requirements (Steffen *et al.*, 2014:186).

3.5.2.2 Semi-structured interviews

In-depth semi-structured interview data constitute the empirical backbone of a lot of qualitative research in the social sciences. There are some basic lessons to be gleaned from the literature that can be applied to semi-structured interview data. And unlike tightly structured interview questionnaires, which tend to elicit short responses, the semi-structured interviews tend to elicit more open-ended, rambling responses (Campbell *et al.*, 2012:5).

Researchers can make use of qualitative design research using face-to-face semi-structured interviews. This method facilitates the collection of rich data on the topic while remaining flexible and participant-guided, making it well suited to exploratory research (Brown *et al.*, 2015:1534).

Semi-structured qualitative interviews are the most common types of interviews because the researcher gets the best of both worlds: a somewhat structured list of questions, so the topic is covered in a coherent manner while maintaining the flexibility to adapt as issues come to light during the interview.

This interview type is particularly useful when exploring a little-known topic because the researcher can follow up interesting issues as they arise. Semi-structured interviews have the drawback of potentially resulting in long and detailed audio data, which requires a significant effort to organise, transcribe and analyse.

Table 3-1: Strength and weaknesses of semi-structured interviews

STRENGTHS	WEAKNESSES
Enables very detailed understanding of the basis for your participants' thinking, feelings, memories and behaviours.	Face-to-face interviews can be expensive and time-consuming to conduct.
Allows for an intensive focus on one individual's perspective.	Depends on your skill as an interviewer to think of the right questions, probe participants' views during the interview and maintain a positive relationship.
You can adjust the direction of the interview as it unfolds in response to what is said.	Interview samples are usually relatively small, raising the risk of not gathering perspectives from a critical segment of the population.
You can clarify and explain aspects of the research without affecting other participants.	Your identity, demeanour and way of framing the interview will affect the replies the participants give.
Relatively high participation rates are possible.	Can be challenging to directly compare data from interviews, as each one is different.
The interviewer can develop initial analytical thinking about participants' answers as they are given, potentially ask follow-up questions to clarify unclear or underdeveloped responses.	
The relative privacy of one-to-one interviews may encourage participants to be more open and honest.	
Can be a positive experience for participants to be intently listened to in an affirming manner for a significant period of time.	

Source: Laurie and Jensen, 2016:174

3.5.2.3 Unstructured interviews

According to Dana *et al.* (2013:513), unstructured interviews are a ubiquitous tool for making screening decisions despite vast literature suggesting they have little validity. Access to an interview could hurt predictive accuracy because exposure to non-diagnostic information is known to dilute valuable information. Unstructured interviews expose interviewers to so many casual observations about the interviewee that have little or unknown diagnosticity that interviewers cannot help but get more information than they can use and thus, they must ignore some cues.

While the parallel collection of quantitative and qualitative data is not new and the growing area of social demography presents an opportunity to broaden the studies and understanding of the different phenomena and additional information that provides the researcher with an opportunity to corroborate and elaborate findings to initiate new investigations (Schatz & Williams, 2012:184).

Cognitive interviewing is a method used to identify problematic survey questions by asking research participants to report what they are thinking either while answering those survey questions or retrospectively.

Because of its relatively short history, most cognitive interviewing research has focused on examining its effectiveness as a valid and objective pretesting tool, and the researchers have tended to evaluate the cognitive interviewing method with other pretesting techniques to see whether problems detected in different pretesting tools are convergent.

The cognitive interviewing methodology builds upon the participants' open discussion and articulation of their thoughts and feelings about the questionnaire that is being presented to them. The validity of non-English cognitive interviews is of a concern among researchers because the technique is built on the communicative norms of Western cultures where directness and openness in expressing a participants' opinion are encouraged (Park *et al.*, 2014:644).

3.6 CONCLUSIONS

Chapter 3 focuses on the research design and methodologies that can be used. The focus is on the three different research paradigms and a brief explanation of each. The chapter begins with the literature on qualitative research (used to collect in-depth details on a particular topic), quantitative (fresh data collection from a large population) and mixed-methods (a combination of the different research methods) approaches and how each of them can be applicable to the research.

The population and sample of the study are explained and literature on the different sampling techniques that can be applied. The chapter concludes by looking at the data collection methods, the administering of a questionnaire to participants and the different interview techniques that can be used to obtain additional information from participants.

According to Davies and Hughes (2015:244), researchers are urged to 'keep it simple' and ensure from the outset the importance of planning a doable and quality research project. Plain language should be used and the researcher should be consistent and keep the continuous focus of the issue at hand, which ultimately would enable the researcher to complete the research project.

The next chapter in our research study focuses on the data and statistical analysis. The data collection instrument, procedure for collecting the data and the ethical consideration related to the data is discussed. Reliability and validity of our data is explained and the analysis which focuses on the frequencies, descriptives, Cronbach Alpha and standard deviation.

CHAPTER 4: DATA AND ANALYSIS

4.1 INTRODUCTION

Chapter 4 discusses the research methodology used in this study. The chapter begins with the purpose of the study, the data collection instrument used, the validity and reliability of the data and then concludes with the statistical analysis and interpretation of the data.

The questionnaire is broken down into four sections. Section 1 relates to the personal background information of the participants, such as their age, ethnicity, highest qualification, job title, gender and years of work experience. Section 2 looks at the participants' personal awareness of computer-related issues at the workplace while Section 3 focuses on the security audit of the participants' environment in their workplace. The last section, Section 4, was only completed by the management teams and mainly focuses on additional information regarding the business buy-in and support of their ICT strategies, ICT costs and their return on investments.

Section 4 is aimed at obtaining a view on what the different entities spend on their security costs per annum, their capacity and skills in response to business challenges as well as any findings that have been identified by both the internal and external auditors regarding their security environment and managements approach in how they go about in resolving these findings.

A copy of the questionnaire has been attached under the Appendixes (Appendix A).

4.2 PURPOSE OF THE STUDY

The main objective of the study is to develop a framework for the ICT departments in the City of Johannesburg on how they can ensure that their computerised environment is secured. The study will enable the researcher to put forward recommendations on what the most important aspects of building a framework for a computerised environment in a metropolitan municipality are.

The research provides a view of the current state of the ICT security within the different entities in CoJ, the different challenges that are faced by officials and their management teams, as well as what measures can be put in place to ensure that the City has ICT platforms and technologies than can improve the municipal service offerings to its residents.

The suggested framework can then be used to ensure that all the ICT strategies of the different entities are aligned, taking into consideration the different industries that they operate in, but most importantly that they are aligned with the overall strategies of the Municipality in fostering and improving service delivery.

4.3 DATA COLLECTION INSTRUMENT

The common measuring instrument used in this research was through the collection of raw data by means of a questionnaire. The questionnaires were distributed to the different entities' ICT departments within the CoJ.

The questionnaire is made up of questions obtained from the Centre for Education and Research in Information Assurance and Security (CERISA) and other questions that are presented to ICT management by the internal and external auditors. The questionnaire is divided into four areas for the participant to respond on their personal background, personal awareness of computer related issues, security audit and the last part is for management to provide additional information relating to their ICT departments. The CIO forum within the Municipality was used to collate additional information from the ICT heads of the different entities through interviews.

The physical questionnaire was printed out and handed over to the ICT management team in the different entities for distribution amongst their team members. Participation in the study was completely voluntary and anonymous. The questionnaires were returned over a period of 2–3 weeks and once completed, handed over to the North-West University's Statistical Consulting Services (SCS) department for the capturing of data and analysis.

In total, 80 questionnaires were issued to the participants and 71 completed questionnaires were received, amounting to a response rate of 88.75%. The remaining nine questionnaires were not received back from the expected participants.

When it comes to sampling, a very important consideration is the size of the sample. It would be disastrous to come to the phase of data analysis and then realise that the sample is too small and that for example, a certain subgroup of the population is not sufficiently represented in the sample. Using a well -designed probability sampling method, larger samples will represent the population better than the small samples and their findings will be more accurate (Maree & Pietersen, 2020:178).

4.3.1 Procedure for data collection

The collection method of the raw data was through a questionnaire and where possible interviews were conducted with the different participants to clarify certain parts of their responses and obtain additional information that was required. The research study made use of a mixture of questions with a five-point Likert scale to ensure that the respondents are accommodated in cases where they are undecided or not sure. There were additional questions for management to further provide context on how they view their ICT Security environment.

4.3.2 Ethical consideration

The approval to conduct research was granted by the research ethics committee of the NWU (approval number: NWU-01381-19-A4). All the participants in the study were informed that their participation is voluntary and that they had the right not to participate in the study. The description of the purpose and objectives of the study formed part of the questionnaire introduction. The following considerations were made in relation to the participants of the research study:

- **Voluntary participation:** The participants will be assured that their participation is entirely voluntary, that they can withdraw at any stage in the research process, and they will furthermore not suffer any consequences if they decided not to participate in this study.
- **Confidentiality and anonymity:** The surveys that will be completed as part of this study, will be anonymous, and the identities of the participants will be treated confidentially.
- **Academic honesty and integrity:** The researcher will present the research study as his own and academic honesty will be maintained in the writing of this thesis. This work will be free from plagiarism, and the original authors of work cited in this

thesis will be referenced appropriately. The researcher intends to express respect and dignity for the participants throughout the entire process, and it will be crucial to respect their human rights and to ensure that no participant will be harm in any way whatsoever. The conduct of the research need to be fair and ethical, so to ensure the overall success of this research study. To ensure an ethical approach matters such as informed consent, voluntary participation, protect from harm, the preservation of privacy and confidentiality will at all times be considered.

4.3.3 Limitations of the study

On the basis of the responses received, the following limitations were identified in the study:

- Participants not being truthful with their responses
- Differences amongst participants in understanding and interpretation
- Participants having difficulty in conveying their feelings and emotions
- Bias from participants who may have a hidden agenda
- Some of the critical questions may be skipped by the participants
- Literacy levels of some of the participants may make the completion of the questionnaire difficult

4.4 RELIABILITY AND VALIDITY

4.4.1 Reliability

The criteria for reliability fall into two distinct categories: trustworthiness and research design. There is a need and value for research students to contribute to the understanding of design studies which are supported by a foundation of a research design that is trustworthy (Kennedy-Clark, 2012:1).

4.4.2 Validity

Validity signifies the level of quality rigour of the research and has a significant impact on the quality of inferences that are generated from the research study (Zachariads et al., 2013:858). For the purposes of these research study, a face-validity test was conducted by sharing the questionnaire with the promoter of the study, a senior lecturer in the Statistical Consultation Services (SCS), as well as the head of ICT Projects within CoJ.

Researchers invest their time in writing scale items that are unambiguous and clear, and item analyses are carried out to select the best items that comprise a measurement instrument. It is often assumed that the items of a measurement instrument will have the same connotations and meanings for all people and therefore the scale will remain invariant in comparisons of people of different classifications (Mulaudzi, 2016:1).

Although several measures of related frameworks are available, construct validation tends to focus on the face and content validity, rather than tests of criterion validity after scale development. Where studies have explored other dimensions of validity, analysis tends to be limited to correlations with measures of managerial frameworks and covariance analyses of factor structure (Philander *et al.*, 2019:105).

4.5 STATISTICAL ANALYSIS

There is a new interest in statistical analysis and summaries of data and these are enforced by the current involvement of statisticians and methodologists to ensure that value can be attained from such analysis. In order to produce a cultural shift in the research community, the change process needs to extend to traditional university training programmes in which research methodology and statistics are taught to future generations of graduate students (Kratochwill & Levin, 2014:234).

According to Carslaw (2014:4), resources that are available for enhanced data analysis are often distributed across many potentially expensive types of specialist software and other proprietary software that can be used for the analysis of data. Globally, access to such specialist software and the knowledge to use are uneven.

One of the main challenges for both information systems and technology specialists as well as business personnel, is how to filter the essential elements of data for the purposes of service delivery. The technical challenges of this data are very real but the managerial challenges even more significant. Hence, a single approach to how this data is handled will continually be short or problematic in finding solutions to the challenge with data management remaining a major challenge for many organisations (Iyamu, 2018:3).

“Under torture, the data readily yield false confession”, these words caution researchers against using statistical results that have been overly influenced by data snooping activities. This warning may well apply equally well to incorrect information that can emerge from applying a statistical method of which important assumptions have been seriously violated (Gutzwiller & Riffell, 2014:1115).

For nearly all scientific studies, it is important to determine a large enough sample size that will give adequate statistical power to detect the desired effect size. Sample size determination and power consideration, therefore, can arise in any scientific endeavours across a variety of fields. It is also an active research area moving along with expanding scientific fields and new design considerations (Ryan, 2015:160).

The classical tools to analyse continuous responses are multiple linear regression models or analyses of variance or covariance, which are all related to the framework of linear modelling with several factors/regressors. When repeated measurements are available for each participant, mixed-effect models that belong to the class of multilevel models are highly recommended (Letue *et al.*, 2018:561).

A questionnaire was distributed amongst the ICT officials within the CoJ, and the responses from the participants have been analysed used the following techniques:

- frequency;
- descriptives;
- reliability (including the means, standard deviations of the factor scores calculated afterwards); and
- t-test (supplemented with Man-Whitney tests in the case of too small sample sizes per group).

4.5.1 Frequencies

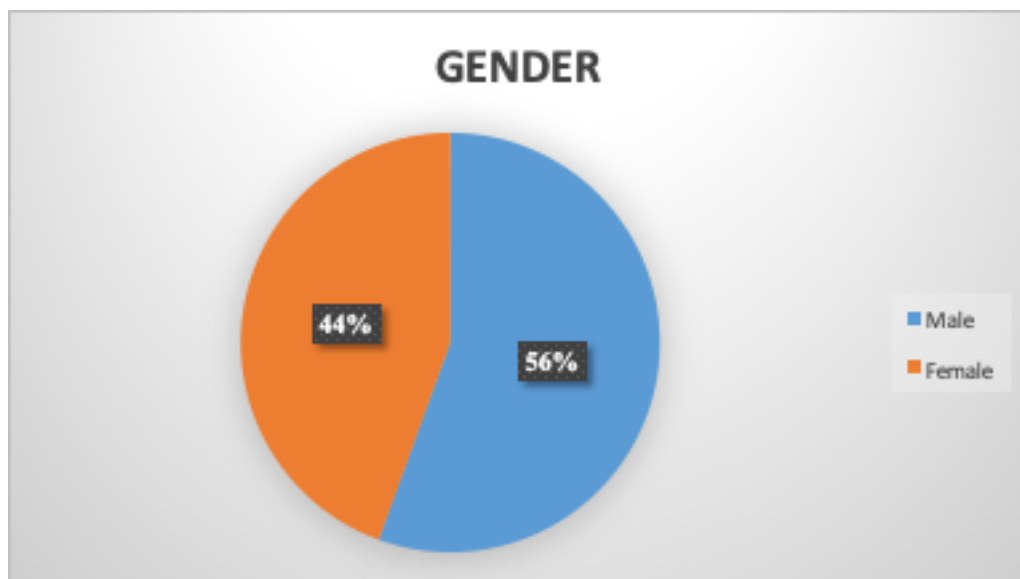


Figure 4-1: Gender statistics

Figure 4.1 on gender shows that out of the total sample, 56% (n=40) of the respondents were male while the remaining 44% (n=32) were female. It must be considered though that due to the sampling method used, these numbers cannot be extrapolated as the overall numbers for the ICT space in the CoJ.

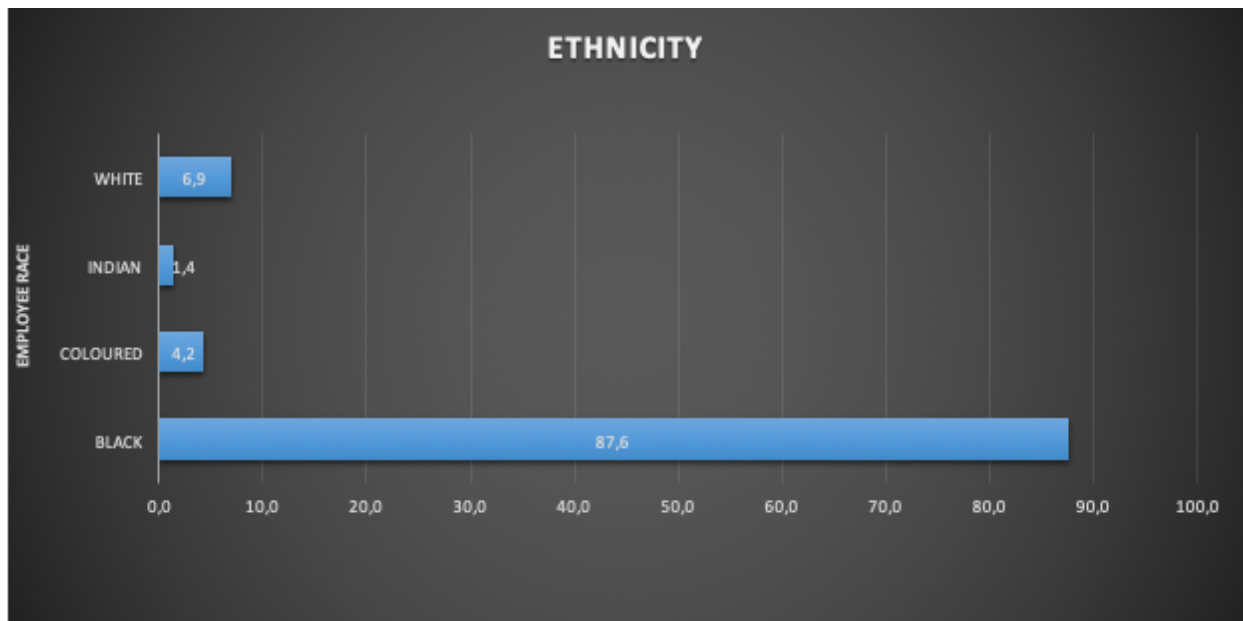


Figure 4-2: Ethnicity

Figure 4.2 on Ethnicity shows the different race groups that participated in our study. The Black Africans (group) is made up of all the African respondents who have used different responses, such as their home languages in the questionnaire. Black Africans were the majority of participants with 87.5% (n=63). The remainder of the population sample (12.5% in total) was divided between Whites (6.9%, n=5), Coloureds (4.2%, n=3 and Indians (1.4%, n=1).

Other biographical questions:

- **Age:** the youngest participant was 22 while the oldest participant was 55 years old. The average age for all the participants was 35.8 years.
- **Years' experience:** the highest number of years of experience was 29 years and the average experience for all the participants was 9.8 years.

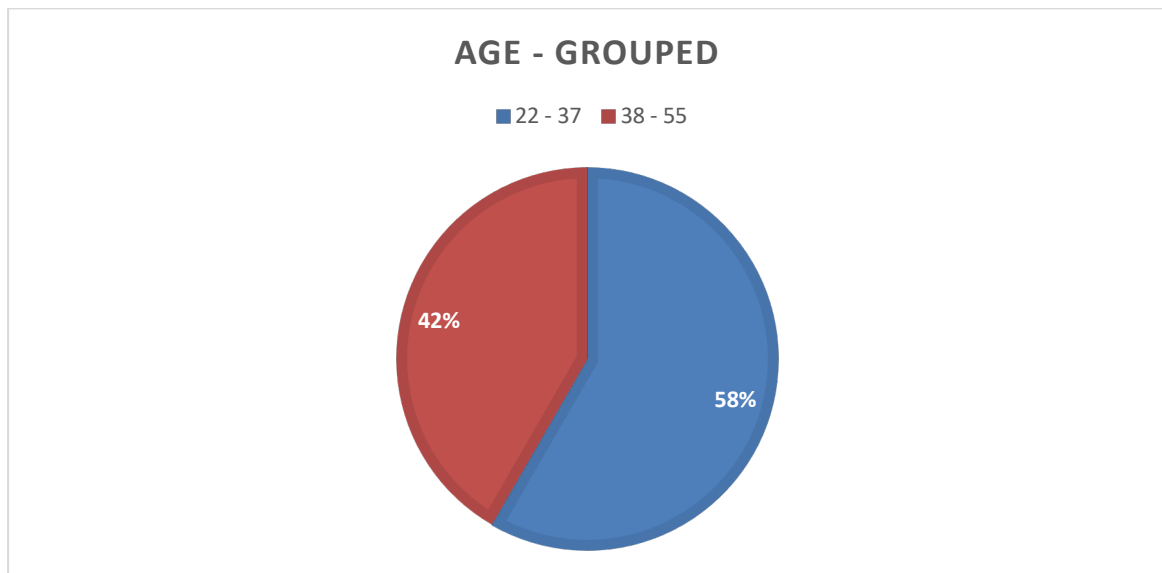


Figure 4-3: Age grouped

Figure 4.3 shows the age groupings that participated in the study. The age group of 22–37 years represents 58% of the study’s total population (n=42), while the age group of 38–55 years is 42% (n=30).

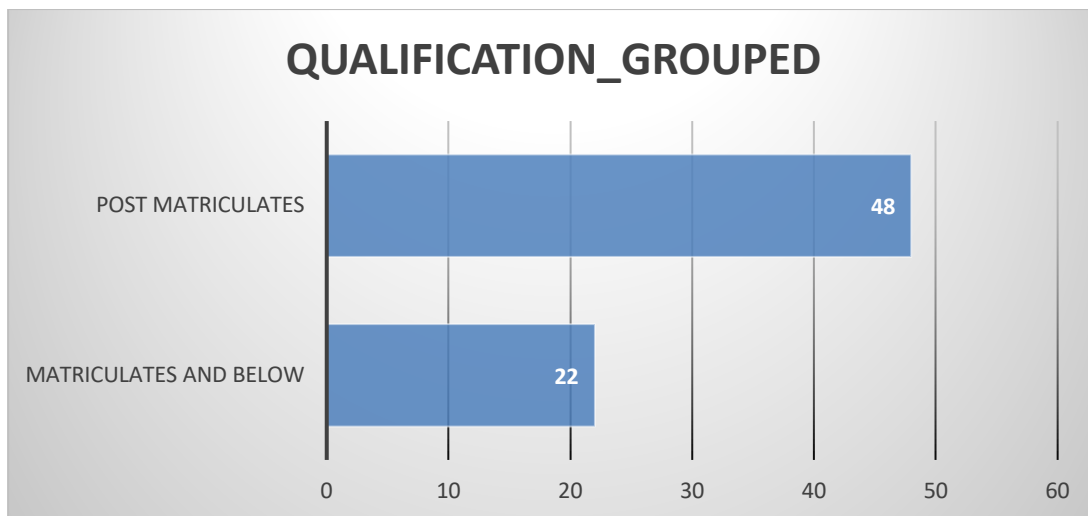


Figure 4-4: Qualification Grouped

Figure 4.4 shows the qualification groupings of the respondents. The post-matriculates group represents 67% of the total population (n=48), while the Matriculates and below group is 42% (n=22). Two participants (n=2) did not complete the qualification part of our questionnaire.

4.5.2 Descriptives

Field (2013:709) provides the following definitions for reliability analysis:

- **Mean:** the measure of central tendency that is simply the average score. To calculate the mean, one simply adds up all of the scores and then divide by the total number of scores one has.
- **Standard deviation:** the square root of the variance to ensure that the measure of average error is in the same units as the original measure. A small standard deviation (relative to the value of the mean itself) indicates that the data points are close to the mean. A large standard deviation (relative to the mean) indicates that the data points are distant from the mean.

The different responses from the respondents in relation to the different section of the questionnaire are looked at. These descriptives are based on responses from Section 2–Section 4 of the questionnaire.

4.5.2.1 Personal awareness

This part of the analysis is derived from Section 2 of the questionnaire and looks at how aware the participants are in relation to the personal experience of a computerised environment.

Table 4-1: Analysis on personal awareness of computer related issues.

Question (A1 - A20)	Strongly Disagree	Disagree	Undecided	Agree	Strongly Agree	Number of Missing	Mean	Std. Deviation
I often use the internet to download music or programs	27.8	19.4	4.2	29.2	19.4	0	2.93	1.550
I regularly check for viruses when I download a file or open an email attachment	9.7	23.6	8.3	34.7	23.6	0	3.39	1.338
My firm uses programs to keep me from looking at Websites that are inappropriate for work	5.6	9.7	11.1	31.9	40.3	1	3.93	1.199
There is nothing wrong with downloading music for free without permission	50.0	25.0	13.9	6.9	4.2	0	1.90	1.140
There is nothing wrong with downloading videos for free without permission	54.2	26.4	9.7	6.9	2.8	0	1.78	1.064
There is nothing wrong with downloading programs for free without permission	44.4	23.6	23.6	6.9	1.4	0	1.97	1.048
I have reported to someone in authority when I was harassed or sent inappropriate material while online	27.8	18.1	30.6	11.1	8.3	3	2.52	1.267

Question (A1 - A20)	Strongly Disagree	Disagree	Undecided	Agree	Strongly Agree	Number of Missing	Mean	Std. Deviation
I often use instant message programs when I'm at work	23.6	16.7	15.3	26.4	18.1	0	2.99	1.458
I often use chat rooms for work purposes	25.0	22.2	13.9	20.8	18.1	0	2.85	1.469
I regularly buy items online	33.3	27.8	6.9	19.4	8.3	3	2.39	1.374
I know how to tell if a website is secure and safe to give information to	12.5	19.4	16.7	22.2	29.2	0	3.36	1.407
I often check for patches or other downloads for my computer to make it safer from hackers	8.3	18.1	18.1	29.2	26.4	0	3.47	1.289
I disconnect from the internet when I am not using it	8.3	13.9	5.6	37.5	34.7	0	3.76	1.295
I have used (or have come in contact with) a firewall or filtering software	5.6	16.7	25.0	27.8	25.0	0	3.50	1.199
I use the same password for everything that needs a password	45.8	22.2	1.4	13.9	16.7	0	2.33	1.565

Question (A1 - A20)	Strongly Disagree	Disagree	Undecided	Agree	Strongly Agree	Number of Missing	Mean	Std. Deviation
I have used the internet to make fun of other people (or say bad things about them) because I knew no one would know it was me who did it	87.5	8.3			2.8	1	1.20	0.710
When the allotted trial time has passed on software, I have downloaded (or borrowed) a 'crack' for it so I could continue using it for free	41.7	23.6	23.6	5.6	4.2	1	2.06	1.132
I am concerned about someone stealing information about myself when I am online	13.9	5.6	13.9	20.8	43.1	2	3.76	1.439
You can't get in trouble for changing someone's website because it's not real.	58.3	19.4	11.1	2.8	5.6	2	1.74	1.138

Table 4.1 provides the breakdown of the responses from the total responses received from the participants to the questions in section 2 of our questionnaire.

The analysis of Table 4.1 looks at the respondents' personal awareness of computer-related issues. These sets of questions look at individual behaviour at work relating to downloads, online chatting and updating/awareness of computer viruses.

The highest mean is 4.15, which indicates that users are aware of the importance of ensuring that their most important work/documents are saved in more than one places. The lowest mean is 1.20 and indicates that users are aware that they should not make use of the internet to make fun or say bad things about the other users.

4.5.2.2 Security audit

This part of the analysis is derived from Section 3 of the questionnaire and focuses on the aspects that relate to the security of the information in the municipality.

Table 4-2: Analysis of security audits within the municipality

Question (A21 - A42)	Strongly Disagree	Disagree	Undecided	Agree	Strongly Agree	Number of Missing	Mean	Std Deviation
The firm has cyber security policies based on industry standards.	5.6	4.2	27.8	30.6	30.6	1	3.8	1.1
The firm has cyber security procedures based on industry standards.	4.2	6.9	25.0	38.9	23.6	1	3.72	1.044
The firm protect sensitive information received from third-parties, with whom data is shared (i.e. encryptions, SSL/TLS connections).	2.8	8.3	22.2	38.9	26.4	1	3.79	1.027
Devices that store or process a third-party firm's sensitive information protected from the internet by a firewall.	2.8	4.2	34.7	30.6	26.4	1	3.75	0.996
The firm has a designated Cyber-Security personnel	13.9	13.9	30.6	26.4	15.3	0	3.15	1.252
Education and awareness programs on cyber-security are regularly performed in our firm	16.7	20.8	25.0	29.2	8.3	0	2.92	1.230
External auditors perform cyber security audits in our firm	5.6	12.5	31.9	31.9	16.7	1	3.42	1.091
Cyber security audits are performed at least once a year	5.6	9.7	37.5	29.2	18.1	0	3.44	1.073

Question (A21 - A42)	Strongly Disagree	Disagree	Undecided	Agree	Strongly Agree	Number of Missing	Mean	Std Deviation
Systems are accessed with a unique username and complex password	1.4	4.2	15.3	38.9	40.3	0	4.13	0.918
Devices that store or process sensitive information have vulnerability scanning performed once a month	5.6	13.9	40.3	27.8	12.5	0	3.28	1.038
Vulnerabilities are remediated in a risk-based priority (highest priority vulnerabilities are fixed first)	4.2	12.5	33.3	33.3	15.3	1	3.44	1.038
Devices that store or process sensitive information have patches updated within industry best practices (i.e.48 Hours) medium/ low risk Patches to be deployed in =<30 days?	2.8	11.1	36.1	31.9	15.3	2	3.47	0.989
Devices that store sensitive information are encrypted	4.2	6.9	20.8	44.4	20.8	2	3.73	1.020
Mobile devices (e.g. smart phones, tablets) that store sensitive information have a remote wipe functionality	6.9	16.7	52.8	15.3	8.3	0	3.01	0.971
Mobile devices (e.g., smart phones, and tablets) that store sensitive information are accessed with a unique username and complex password	6.9	16.7	22.2	30.6	22.2	1	3.45	1.216

Question (A21 - A42)	Strongly Disagree	Disagree	Undecided	Agree	Strongly Agree	Number of Missing	Mean	Std Deviation
The firm has a Computer Incident Response Team (CIRT) to respond to cyber-attacks	8.3	18.1	36.1	19.4	18.1		3.21	1.186
The firm has a formal process to respond to cyber-attacks	9.7	11.1	38.9	22.2	16.7	1	3.25	1.168
The firm requires a 2-factor authentication for remote access (e.g. a token used in addition to a username and password for a VPN login)	5.6	4.2	36.1	37.5	16.7	0	3.56	1.005
The firm performs industry standard monitoring on devices that store or process sensitive Information	2.8	12.5	33.3	36.1	15.3	0	3.49	0.993
The firm controls web access based on the risk (e.g. reputation, content, and security) of the sites being visited (E.g. Web Proxy controls)	1.4	11.1	25.0	44.4	18.1	0	3.67	0.949
The firm actively participate in cyber-Intel sharing forums (e.g.ISAC, Infraguard)?	15.3	11.1	51.4	9.7	12.5	0	2.93	1.155
The firm regularly performs phishing e-mail testing on its employees	9.7	11.1	45.8	16.7	16.7	0	3.19	1.146

Table 4.2 provides the breakdown of the responses from the total responses received from the participants to the questions in section 3 of the questionnaire.

The analysis of Table 4.2 focuses on the respondents' views on matters which may result in audit findings from both internal and external auditors in the municipality. The questions focus primarily on issues that relate to cybersecurity, system access, encryption on devices and any authentication that is required to access company systems.

The highest mean is 4.13, which indicates that participants agree and are in favour of the municipality making use of unique usernames and complex passwords for accessing the systems. The lowest mean of 2.92 indicates that participants are not convinced that enough is being done on cyber-security education and awareness programs that are performed regularly in their municipality

4.5.2.3 Questions relating to management only

This part of our analysis is derived from Section 4 of our questionnaire and looks at providing further information relating to the view of management on the business buy-in in the ICT strategy as well as whether they feel that the organization is deriving benefits from such investments.

Table 4-3: Analysis of management related questions

Question (A43 - A51)	N	Mean	Standard Deviation
On a scale of 1–10 (1=bad & 10=good), do you have business buy-in and support towards the overall ICT Strategy?	32	6.38	2.366
On a scale of 1–10 (1=bad & 10=good), would you say business is deriving benefits from the costs attributed to ICT Security (ROI)?	32	5.91	2.582
On a scale of 1–10 (1=bad & 10=good), do you have enough capacity and skills within	35	4.83	2.629

Question (A43 - A51)	N	Mean	Standard Deviation
your ICT department to address issues relating to ICT Security?			
On a scale of 1–10 (1=bad & 10=good), how secure is your overall ICT Security platform within the organisation?	35	5.86	2.366

Table 4.3 provides the breakdown of the responses from the total responses received from the participants to the questions in section 4 of the questionnaire.

The mean of “business buy-in and support towards the overall ICT strategy”, was the highest with 6.38 which shows that management is leaning towards having good buy-in and support from the business with regard to their overall ICT Strategy.

The question relating to having the required levels of skills/capacity to address ICT security issues had the lowest mean with 4.83 which demonstrates that management is leaning towards not having enough skills and capacity within their areas of the business to deal with issues relating to ICT Security.

4.5.3 Cronbach's alpha, mean and standard deviation

Field (2013:709) provides the following definitions for reliability analysis:

- **Cronbach's alpha** – used to measure the internal reliability or consistency of the questionnaire. The guideline value is 0.7, but 0.5 can be used although its interpretation should be handled with caution.

Cronbach's basic equation for alpha:

$$\alpha = \frac{n}{n-1} \left(1 - \frac{\sum V_i}{V_{test}} \right)$$

n = number of questions

V_i = variance of scores on each question

V_{test} = total variance of overall scores (not %'s) on the entire test

For the purposes of the analyses, the different questions in the questionnaire were grouped into the following groups:

- **Questions 4, 5, 6** – Free downloads without permission
- **Questions 9, 10** – Use of chatrooms
- **Questions 21, 22, 25** – Cybersecurity policies, procedures and standards
- **Questions 23, 24** – Protection of company information shared with third parties
- **Questions 26, 27, 28** – Cybersecurity awareness (organisational)
- **Questions 30, 31** – Vulnerability scanning and assessment
- **Questions 33, 34, 35, 39** – Encryption and Protection
- **Questions 36, 37** – Cyber-attacks response processes
- **Questions 29, 38** – System access security
- **Questions 43, 45** – Business buy-in and ROI
- **Questions 47, 51** – Skills and a secure computer environment

Table 4-4: Cronbach alphas and descriptive statistics of factors

Names	Questions	Cronbach Alpha	Mean	Std Deviation
Free Downloads	4, 5 & 6	0,89	1,88	0,98
Chatrooms	9 & 10	0.654	2,92	1,26
Cyber Security	21, 22 & 25	0.817	3,54	0,97
Information Protection	23 & 24	0.633	3,77	0,87
Cyber Security Awareness	26, 27 & 28	0.773	3,17	0,88
Vulnerability	30 & 31	0.73	3,34	0,95
Encryption and Protection	33, 34, 35 & 39	0.849	3,44	0,82
Cyber Attack Responses	36 & 37	0.815	3,23	1,08
Secure Access	29 & 38	0.662	3,78	0,74
Business Buy in and ROI	43 & 45	0.790	6,04	2,25
Capacit/Skill and secure environment	47 & 51	0.70	5,34	2,31

Table 4.4 shows the Cronbach Alpha, the mean and standard deviation for each of the groupings as per the explanation above.

The Cronbach alpha values for all the grouped questions on the questionnaire are between 0.633 and 0.89. The lowest Cronbach is 0.633 for Information Protection, and the highest one is 0.89 for Free Downloads. These constructs are considered reliable as all of them are above the guideline value of at least 0.5.

4.5.4 Comparative analysis

Field (2013:709) provides the following definitions:

- **Effect size** – the measure which helps to describe the practical significance of the difference between the means of the two groups. The guideline for the effect size is as follows:
 - **0.2 small** – no practically significant difference
 - **0.5 medium** – practically visible difference
 - **0.8 large** – practically significant difference

For further analyses, ethnicity was grouped into Africans (87.6%) and the Others which were made up of Coloureds, White and Indians (12.4%).

- **T-test** – testing for differences between two groups.
- ***P-value** – reported for completeness sake but will not be interpreted since a convenience sample instead of a random sample was used.
- **Man-Whitney** – commonly used when the group size is smaller than 20.

Table 4-5: Independent T-test and Man-Whitney for Ethnicity

Questions Grouped	Ethnicity Grouped	N	Mean	Std. Deviation	T-test		Man-Whitney	
					p-value	Effect size	p-value	Effect size
Free Download	Africans	63	1,91	1,01	0,48	0.20	0.792	0.03
	Others	9	1,70	0,75				
Chat Rooms	Africans	63	2,95	1,25	0,58	0.20	0.612	0.06
	Others	9	2,67	1,41				
Cyber Security	Africans	63	3,61	0,94	0,20	0,48	0.225	0.14
	Others	9	3,07	1,10				
Information Protection	Africans	62	3,85	0,84	0,08	0,69	0.077	0.21
	Others	9	3,22	0,91				
Cyber Security Awareness	Africans	63	3,26	0,84	0,09	0,66	0.098	0.19
	Others	9	2,58	1,02				
Vulnerability	Africans	63	3,44	0,95	0,00	0,81	0.007	0.32
	Others	9	2,67	0,56				
Encryption and Protection	Africans	63	3,52	0,81	0,02	0,84	0.019	0.28
	Others	9	2,84	0,71				
Cyber Attack Response	Africans	63	3,33	1,06	0,03	0,78	0.029	0.26
	Others	9	2,50	0,94				
Secure Access	Africans	63	3,81	0,72	0,42	0,29	0.434	0.09
	Others	9	3,56	0,88				
Business Buy in & ROI	Africans	29	6,00	2,36	0,74	0,13	0.961	0.01
	Others	5	6,30	1,64				
Capacity/ Skills and Secure Environment	Africans	33	5,38	2,43	0,50	0,16	0.883	0.02
	Others	4	5,00	0,71				

Table 4.5 shows us that there are practically visible and/or practically significant differences between Africans and other groups for Information Protection ($d=0.69$ and $r=0.21$), Cyber Security Awareness ($d=0.66$ and $r=0.19$) Vulnerability ($d=0.81$ and $r=0.32$), Encryption and Protection ($d=0.84$ and $r=0.28$) as well as Cyber Attack Response ($d=0.78$ and $r=0.26$). The means for Africans always being higher than the means of Others.

Table 4-6: Independent T-test for Age Group

Questions Grouped	Age Grouped	N	Mean	Std. Deviation	T-test	
					p-value	Effect size
Free Downloads	22 - 37	42	2,127	1,041	0,01	0,56
	38 - 55	30	1,544	0,785		
Chat Rooms	22 - 37	42	3,024	1,239	0,40	0,20
	38 - 55	30	2,767	1,298		
Cyber Security	22 - 37	42	3,603	0,932	0,54	0,14
	38 - 55	30	3,456	1,038		
Information Protection	22 - 37	41	3,841	0,825	0,41	0,19
	38 - 55	30	3,667	0,922		
Cyber Security Awareness	22 - 37	42	3,143	0,875	0,73	0,08
	38 - 55	30	3,217	0,907		
Vulnerability	22 - 37	42	3,369	0,870	0,77	0,07
	38 - 55	30	3,300	1,055		
Encryption And Protection	22 - 37	42	3,494	0,751	0,50	0,15
	38 - 55	30	3,355	0,918		
Cyber Attack Response	22 - 37	42	3,333	0,973	0,35	0,21
	38 - 55	30	3,083	1,211		
Secure Access	22 - 37	42	3,778	0,693	0,95	0,01
	38 - 55	30	3,789	0,814		
Business Buy in & ROI	22 - 37	14	5,929	1,838	0,80	0,08
	38 - 55	20	6,125	2,539		
Capacity/Skills and Secure Environment	22 - 37	17	5,853	2,720	0,23	0,35
	38 - 55	20	4,900	1,847		

Table 4.6 shows, based on the effect sizes, no practical significant differences for age groups. The most substantial effect being for free downloads ($d=0.56$) which demonstrates a practically visible difference in the views of the different age groups with the younger group disagreeing to the statements and the older groups disagree leaning towards strongly disagreeing.

Table 4-7: Independent T-test for Experience Group

Questions_Grouped	Experience_Grouped	N	Mean	Std. Deviation	T-test	
					p-value	Effect size
Free Downloads	0 - 10	44	2,038	1,050	0,02	0,47
	11 - 29	27	1,543	0,642		
Chat Rooms	0 - 10	44	2,841	1,209	0,55	0,14
	11 - 29	27	3,037	1,379		
Cyber Security	0 - 10	44	3,515	0,873	0,80	0,06
	11 - 29	27	3,580	1,149		
Information Protection	0 - 10	44	3,761	0,803	0,97	0,01
	11 - 29	26	3,769	0,992		
Cyber Security Awareness	0 - 10	44	3,199	0,910	0,68	0,10
	11 - 29	27	3,111	0,861		
Vulnerability	0 - 10	44	3,386	0,834	0,62	0,11
	11 - 29	27	3,259	1,130		
Encryption And Protection	0 - 10	44	3,485	0,702	0,50	0,15
	11 - 29	27	3,335	1,000		
Cyber Attack Response	0 - 10	44	3,136	0,930	0,46	0,17
	11 - 29	27	3,352	1,300		
Secure Access	0 - 10	44	3,788	0,686	0,86	0,04
	11 - 29	27	3,753	0,840		
Business Buy in & ROI	0 - 10	17	5,618	2,140	0,28	0,37
	11 - 29	17	6,471	2,335		
Capacity/Skills and Secure Environment	0 - 10	20	5,725	2,505	0,27	0,34
	11 - 29	17	4,882	2,027		

Table 4.7 shows, based on the effect sizes, no practical significant differences for experience groups. The most considerable effect being for free downloads (0.47) which demonstrates a practically visible difference in the views of the different experience groups with the less experienced group disagreeing to the statements and the more experienced group strongly disagreeing but leaning towards disagreeing.

Table 4-8: Independent T-test for Qualification Group

Questions Grouped	Qualification Grouped	N	Mean	Std. Deviation	T-test	
					p-value	Effect size
Free Downloads	Matriculates and below	22	1,879	0,917	0,99	0,00
	Post Matriculates	48	1,882	1,035		
Chat Rooms	Matriculates and below	22	3,045	1,290	0,59	0,14
	Post Matriculates	48	2,865	1,275		
Cyber Security	Matriculates and below	22	3,333	0,954	0,21	0,32
	Post Matriculates	48	3,653	0,992		
Information Protection	Matriculates and below	22	3,591	0,796	0,28	0,26
	Post Matriculates	48	3,823	0,884		
Cyber Security Awareness	Matriculates and below	22	3,114	0,996	0,76	0,07
	Post Matriculates	48	3,188	0,847		
Vulnerability	Matriculates and below	22	3,250	0,686	0,59	0,11
	Post Matriculates	48	3,365	1,051		
Encryption And Protection	Matriculates and below	22	3,343	0,631	0,51	0,14
	Post Matriculates	48	3,468	0,907		
Cyber Attack Response	Matriculates and below	22	3,068	0,942	0,37	0,20
	Post Matriculates	48	3,302	1,157		
Secure Access	Matriculates and below	22	3,727	0,710	0,70	0,10
	Post Matriculates	48	3,799	0,746		
Business Buy in & ROI	Matriculates and below	7	5,929	2,188	0,88	0,06
	Post Matriculates	27	6,074	2,303		
Capacity/Skills and Secure Environment	Matriculates and below	9	5,778	2,425	0,54	0,24
	Post Matriculates	28	5,196	2,295		

Table 4.8 shows only practically insignificant differences.

4.6 CONCLUSIONS

Chapter four begins with looking at the purpose of the research study and the data collection instrument. The ethical considerations and the limitations to our study are also identified.

The reliability and validity of our data is explained in relation to the steps undertaken for the purposes of the research study. The chapter is completed by looking at the statistical analysis which focuses on frequencies, descriptives, Cronbach Alpha and standard deviation.

Comparative analysis is done to determine the effect size, T-test, P-value and Man-whitney. The data for the comparative analysis was drawn from the Ethnicity, Age, Experience and Qualification Group.

According to Letue *et al.* (2018:561), the behaviour of one participant may have some fluctuations from one answer to the other. These sources of fluctuation are called intra-individual variability. Research participants are individual people in their own rights and therefore, it should not be expected of them to give the same responses to the same set of questions in the research.

The next chapter focus on the actual framework for a secure computing environment. The research study looks at the key aspects of the framework and how the managerial framework is developed through from the research objectives, literature review, research design and statistical analysis.

CHAPTER 5: FRAMEWORK FOR A SECURED COMPUTERISED ENVIRONMENT

5.1 INTRODUCTION

This chapter looks at the design of the framework that is required for a secured computing environment in a metropolitan municipality. The chapter starts by looking at the definition of a framework and how it can or should be applied in the research studies. The different enablers that contribute to a secure computerised environment are each explained in detail on how they contribute to the framework before the chapter is summarised.

The assignment by government officials of reinventing government has been a primary theme since the 1990s, with governments all over the world trying to improve their systems for public service delivery. The accelerated growth of ICT systems is revolutionising the way government services are delivered nowadays. The government services and processes can be better managed by using a variety of ICT platforms, applications and services.

Compelling cases have been made worldwide, including in South Africa, for more integrated approaches to environmental governance. There is no one set of institutional arrangements that can solve all types of collective problems. To be effective, organisations and their systems need to be designed in ways that are compatible with particular types of problems (Muller, 2007:18).

The successful initiatives and implementation of e-government at the municipal level have facilitated municipalities in terms of revenue generation, achieving transparency, efficient service delivery, and increased satisfaction amongst citizens.

Public services are rapidly becoming dependent on ICT-based services – automatic teller machines, voice response systems, traffic information, etc. Almost all of these ICT systems make considerable demands from the users with regard to the ability to read and write, interpret information quickly and make decisions, and for some, to respond within a given period of time. The ability to retrieve information in an efficient way is crucial to being able to lead an active life (Sandberg *et al.*, 2005:230).

5.2 A FRAMEWORK FOR A SECURE COMPUTING ENVIRONMENT

Twum-Darko (2014:512) mentions that in order to improve productivity, the application of the transformational e-government (TeG) needs to be implemented and adopted to address the cultural and organisational barriers which have hindered the realisation of service delivery in the local government spheres. TeG is further defined as “the exploitation of e-government such that benefits can be realised” i.e. the use of computer-based information and communication technologies (ICT) to enable radical improvement to the delivery of services to citizens.

According to Thinyane *et al.* (2015:241) with reference to the context of participation in government, questions have been posed as to whether e-government systems can help increase the accountability of public governance.

Proponents of the use of technology for development cite the following reasons for their use:

- increased penetration of mobile devices;
- availability of mobile internet; and
- the potential of technology to leapfrog over other developmental challenges.

The Find & Fix app allows citizens to report problems such as potholes to the Johannesburg Road Agency (JRA). The app utilises geotagging to identify the location of the pothole, which initiates a series of processes that result in the pothole being repaired far more quickly than a call to the contact centre. While traditional contact centre communication provides communities with the opportunity to report a problem, incident or an event, they are often regarded as challenging and inconvenient due to long waiting queues, redirects, dropped calls and more.

With nearly 200 smart city apps around the world, a citizen-reporting app allows the public to report an incident at the moment, without any hassles and the unpleasantness associated with contact centres (Frankson, 2016:78).

According to Kaselowski *et al.* (2010:333) IT is becoming ever-increasingly important in the way's municipalities manage and use their information for decision-making purposes. Municipal service delivery is absolutely dependent on accurate information as well as the related IT infrastructure that captures, stores and transmits information. It is critically

important to ensure that information-related IT is adequately governed. This will ensure that the correct information is always available to the correct entities, resulting in better delivery of services to citizens of South Africa.

Accurate information plays a fundamental role in any municipality. Without it, sound decision-making becomes difficult and risky. Further, most business processes today depend on reliable information and related information technologies (IT). Thus, it is important to properly manage and protect the use of information and IT within the municipality.

IT has advanced rapidly over the last few decades, and this rapid development of IT poses several threats to the information of a municipality if the IT infrastructure, including its systems, processes and the people who work with it, is not properly governed and planned for. As a result, proper IT governance has become increasingly important in most municipality.

Coleman (2014:179) explains that prior to the colonisation of the African continent in general, and South Africa in particular, social organisation was characterised by a number of tribal regimes based on patriarchy and ascriptive norms. Each tribe, to date, has had a traditional leader who was the central figure. The traditional leadership is the highest authority in the territory, and the majority of South Africans, especially in the rural areas, continue to owe allegiance and support to this institution of traditional leadership.

There are several challenges confronting traditional governance in Africa. These challenges revolve around the issue of record-keeping, management, accessibility, as well as the appropriate coding, packaging and dissemination of indigenous knowledge, as indicated earlier. These challenges extend to networking and connectivity for the purpose of monitoring, counselling, and sharing experiences and information. There is great potential in computer-mediated tools to alleviate some of these challenges.

According to Unathi *et al.* (2017:439), the Auditor-General South Africa (AGSA) states that IT controls within local government are developed without considering the IT risks associated with them and are not informed by the threats and weakness assessments. In trying to address the issues identified by AGSA with regard to sound IT governance, various municipal frameworks for the sound governance of IT have been developed.

It is, however, during the implementation of the aforementioned frameworks, where risk management remains an issue as these frameworks frequently fail to address how risk management activities, in particular risk assessment, can be achieved in local government. ICT departments within municipalities should have open, honest and constructive discussions about managing risks that relates to their strategic objectives and ensure that their strategic formulation and implementation is based on such risk discussions.

Legislation tabled subsequent to the 1994 elections has provided rules, controls and processes in pursuit of equitable allocation of resources across the three spheres of government, with a focus on correcting the imbalances created by the apartheid system. The legislation may be sound and can be implemented to the latter, yet often fails to yield the best results for reasons as simple as having a span of control that is too large to enable fair consideration for all variables and options (Kaiser & Smallwood, 2014:94).

The development of a vision of an information society should be directed towards citizens needs rather than echoing those of other nations. This vision of the information society should essentially seek to ensure that the advantages offered by the information revolution reach down to every level of society and achieve an optimum balance between individuals and social groups, communities and societies as is practically possible (Pillay, 2002:115).

According to Graham *et al.* (2015:72), technical communication scholars are very familiar with the long-standing problem of inclusion in science, technology, engineering and maths policy disputes. Recent literature and studies have offered multiple and conflicting normative versions for the most ethical and practical models for policy decision making.

This issue is the focus in terms of determining how to include the marginalised voices of nonexpert classes in policy decision making. The long history of governmental agencies, in concert with technical experts, making policy decisions without public input strongly suggests the need for an increasingly democratic approach to those decisions.

5.3 DEVELOPMENT OF THE FRAMEWORK

Local governments, in addition to being close to citizens and business, constitutes for the primary (or even unique) representation of government. The relationship of citizens and local authorities tends to be one based on proximity as the interests at stake for both parties are clearly entwined concerning issues such as public services, urban development, school planning, environmental concerns and local politics. It is at this level of local government that the impact of ICT on the relationship between governments and citizens can be at its most effective and efficient (Misuraca, 2007:94).

The temptation nowadays is to limit ICTs to the computer and exclude other technologies such as radio, television and print. These technologies are readily available in homes and offices and have proven to be effective and inexpensive ways of enabling high-quality information to reach remote clientele and overcome geographical and cultural hurdles (Aderinoye, 2008:607).

5.3.1 Theoretical framework

According to Grant and Osanloo (2014:12) the theoretical framework is one of the most important aspects in the research process yet is often misunderstood by doctoral candidates as they prepare their dissertation research study. The importance of theory-driven thinking and acting is emphasised in relation to the selection of a topic, the development of research questions, the conceptualisation of the literature review, the design approach, and the analysis plan for the dissertation study.

The importance of utilising a theoretical framework in a dissertation study cannot be stressed enough. The theoretical framework is the foundation from which all knowledge is constructed (metaphorically and literally) for a research study.

It serves as the structure and support for the rationale for the study, the problem statement, the purpose, the significance, and the research questions. The theoretical framework provides a grounding base, or an anchor, for the literature review, and most importantly, the methods and analysis.

According to Adom *et al.* (2018:438) a framework is the 'blueprint' or guide for research, and it's based on an existing theory in a field of inquiry that is related and/or reflects the hypothesis of a study. It is a blueprint that is often 'borrowed' by the researcher to build his/her own house or research inquiry. It serves as the foundation upon which research is constructed.

Green (2016:2) clarifies that it is a matter of interpretation as to when concepts become organised and interrelated enough to be deemed theories which might explain as to why the two terms are utilised interchangeably when referring to frameworks.

The term theoretical framework should be used when research is underpinned by one single theory and that a conceptual framework draws on concepts from various theories and research findings to guide a research project.

According to Nwagwu and Ibeku (2016:36), innovation is a means of devising and/or applying existing technologies, methods, and ideas to achieve better solutions to the problems of human society. It involves the application of creativity to meet both existing and new market needs through the development of more effective products, processes, services, technologies or ideas.

Based on the research objectives in Chapter 1, the literature review, the questions grouping from the questionnaire and the statistical analysis thereof, the following drivers as key to the formulation of the framework were identified:

- ICT departmental roles
- Types/levels of skills required
- Technology platforms (software and hardware)
- Applications
- Governance
- ICT Strategies

5.3.2 ICT department's role

Mawela *et al.* (2017:159) argues that the ICT department within municipalities are not receiving the necessary attention due to the low profile it holds. ICT was not seen as an important department like the service departments (e.g. water, electricity and waste departments). Even in the support departments, the ICT department also did not have much power as compared to the more established functions (e.g. audit and finance).

The head of the ICT department has to change the perception of ICT and its role within the municipality. If they do not, ICT will have little or no impact in the municipality. ICT is not a backroom function but rather part and parcel of trying to achieve a responsive and accountable local government. The raising of the profile of ICT will also be dependent on where the department is placed in the municipality structure.

According to Mokhele and De Beer (2007:62), the revolution of ICT has facilitated the globalisation of the economy, business, finance and culture. The application of ICT services within the government can be divided into: access of information, transaction services and citizen participation. ICT departments play a vital role in enabling the modernisation of government and its services.

ICT allows both individual and companies the opportunity to interact with government 24/7 using the different means of communications such as: desktops, laptops, cell phones, telephones and self-service kiosks.

Scholl and AlAwadhi (2016:28) argue that along with the idea of service integration and standardisation; an ICT department should be focused on smoothing and streamlining processes, notably including those that span organisational borderlines. Refocusing from departmental administrative orientations and more towards a process model and its outcome including a quality-oriented service culture is expected to foster a major shift in understanding the public-sector service obligation. This is also viewed as a prerequisite for speeding up processes as well as for balancing business and ICT needs.

5.3.3 Level and type of skills required

South Africa faces human capital development challenges in building the inclusive information society. One of the key challenges is the shortage of skilled ICT graduates in the country aggravated by the 'brain drain' of skilled ICT personnel and other professionals to developed countries (e.g. Australia and Germany) and the turnover from the public to the private sector. There is a shortage of skilled IT staff in the public sector compared to the private sector in South Africa (Murenzi & Olivier, 2017:146).

Indian information technology has come a long way since the 1990s and has grown from US\$150 million in 1991-1992 to US\$150 billion in 2016 –2017. Most of this growth and success has been attributed to the accessibility of low-cost technical resources, skilled manpower, lower salary and project execution from India. Profit revenue was based on the number of projects executed and the number of resources deployed. The biggest challenge is not just attaining growth but to sustain it. To ensure sustained growth of Indian IT organisations, a new leadership climate which will inspire the workforce to voluntarily and creatively add value is required (Patrick, 2018:2).

According to Chisango and Lesame (2017:57), the national Department of Basic Education should include ICT skills in the curriculum for both primary and high school learners. It should also be investigated whether subjects such as Computer Application Technology and Information Technology should not be made compulsory in school.

Access to essential ICT equipment, including computers and Internet access, should be ensured at schools. This could be coupled with a computer literacy programme for educators, together with the provision of the software required in teaching and learning. In addition, measures to protect ICT infrastructure should be implemented. Provincial education departments should also investigate the possibility of conducting ICT literacy programmes for teachers at schools.

Information is widely recognised as a valuable commodity. This is particularly true in organisations where information is a crucial resource for organisational survival and success. Information is recognised by managers and municipalities as a crucial resource for attaining organisational goals and improving the performance of the organisation. There has been a positive correlation that exists between management success and sufficient information needs assessment, gathering and use.

In municipalities, managers are people who occupy strategic positions and play instrumental roles in monitoring the environment (internally and externally), processing information, generating new knowledge for the organisation and work through others to initiate change and improve organisational performance (Naidoo & Nsibirwa, 2015:3).

In attempting to define IT skills, Twinomurinzi *et al.* (2017:217) explain that there is a challenge of where to set the boundaries in order to create a succinct definition. ICT can now be found in hospitals, schools, rural homes, villages and in the most unexpected places that we can imagine. By its nature, the ICT discipline means that with every crossing between ICT and domain area, a new form of ICT is created, which brings along the challenges of the skills-set required to support the emergence of the new competence.

This challenge is arguably one of the key reasons that there is a higher demand for ICT skills that enables the cross between ICT and other domain areas. Recruitment agencies in South Africa support the suggestion that skills in ICT, particularly in software development, have been the highest in demand and have continued to show growth for more than five years.

In an era where the words ‘fourth industrial revolution’ are being thrown around alongside the latest development in technology, skills in cloud computing, cybersecurity, IoT, artificial intelligence and digitisation are sure to be the buzz-words for anyone looking into making an investment in the ICT skills for next ten years or so.

Smith (2012:39) provides the following list, which gives an indication of the type and level of expertise of ICT skills that are required to move towards and manage a functional ICT framework in a municipality:

- **Information management** – the overall management of information, as a fundamental business resource, to ensure that the information needs of the business is met.
- **Business risk management** – the planning and implementation of organisation-wide processes and procedures for the management of operational risk.
- **Information security** – the management of, and provision of expert advice on, the selection, design, justification, implementation and operation of information security controls and management strategies to maintain the confidentiality,

integrity, availability, accountability and relevance compliance of information systems.

- **Security administration** – authorisation and monitoring access to IT facilities or infrastructure in accordance with organisational policies.
- **Information assurance** – protection of systems and information in storage, processing, or transit from unauthorised access or modification.
- **Systems architecture** – specification of systems architectures, identifying the components needed to meet the present and future requirements.
- **Continuity management** – the provision of service continuity planning and support.
- **Network design** – production of network design and design policies, strategies, architectures and documentation, covering voice, data, text, email, facsimile and image, to support business requirements and strategies.
- **Network operations** – day-to-day operation and maintenance of networked systems to ensure that the communication needs of the business are met
- **Programming/software development** – design, creation, testing and documenting of new and amended programs from supplied specifications in accordance with agreed standards.
- **Website specialist** – design, creation, testing, implementation and support of new and amended collections of pages of information on the world wide web or an intranet or extranet.
- **Project management** – management of projects involving the development and implementation of business processes to meet business needs within the agreed parameters of cost, time and quality.
- **Configuration management** – systematic management of information relating to the documentation, software, hardware and firmware assets of an organisation.
- **Change management** – management of all changes to the components of a live infrastructure, from requests for change (RFC) through to implementation and review, to support the continued availability, effectiveness and safety of the infrastructure.
- **Capacity management** – management of the capability and functionality of hardware, software and network components to meet current and predicted needs in a cost-effective manner.

- **Availability management** – overall control and management of services and their availability to ensure that all services meet all of their agreed availability targets.
- **Financial management for ICT** – overall financial management, control and stewardship of ICT assets and resources used in the provision of ICT services, ensuring that all governance, legal and regulatory requirements are complied with.
- **Management and operations** – management and operation of the ICT infrastructure and the resources required to plan for, develop, deliver and support properly engineered ICT services and products to meet the needs of a business.

5.3.4 Software

The performance of municipalities is embedded in its ability to ensure that it has the necessary management tools in place to provide service delivery to the communities that it serves.

All municipalities are required to prepare and submit their annual financial statements for auditing within two months of the financial year-end. One of the reasons for non-compliance with MMFA is the lack of capacity, staff constraints and software/tools that can enable the municipalities to implement the Generally Recognised Accounting Practices (GRAP).

Section 24 of the MFMA requires a municipal council to approve its annual budget before the commencement of its budget year. Furthermore, MFMA circular 48 requires that such budgets be prepared in the prescribed format. However, constraints such as skills and staff shortages hamper municipalities from meeting these legislative requirements.

5.3.5 Hardware

Table 5-1 refers to the alignment of the business objectives of a municipal entity as required by principle 5.2 of the King III report. Table 5-1 refers to both hardware and applications requirements.

Table 5-1: Municipal's entities requirements for hardware

Imperative	Operational Requirements	ICT Environment	Clusters Impacted
Affordability	Public sector entities require ICT costs to be low and are focused on value for money. The benefits received from the ICT environment should outweigh the costs. Costs of ownership and operating costs should be low in order to utilise taxpayers' money efficiently in transforming it into tangible outcomes for society.	The cost of ownership of particular ICT software and hardware needs to be as low as possible. This includes the initial purchase price, annual license fees and the costs associated with upgrades and maintenance.	Applications Hardware Networks
Agility	The ICT systems should be able to adapt to changes in political power, restructuring possibilities and changes in the economy. ICT should also be able to adapt to easier methods of interactions with the public.	The hardware and applications need to facilitate various systems since a public sector entity is diverse in its trade and has various stakeholders. ICT should be easy to upgrade and maintain the system	Applications Hardware
Reliability	Systems need to function as intended at all times, thereby being available, effective and efficient.	The systems should be of a function of reliable quality to avoid malfunctioning. The systems should also be able to adjust to unexpected changes with minimal damage. A detailed contingency plan should be in place. A continual monitoring	Applications Hardware Networks

		system that monitors the availability of systems	
Security	Unauthorised access to the personal data of citizens should be prevented.	Data must be kept in a valid, accurate and complete manner. Appropriate firewalls, anti-virus programs and facilitation of administrators' rights should be in place	Applications Hardware Networks

5.3.6 Applications

According to Mzekandaba (2018:1) the race to bring municipal services closer to the people is heating up, as more local government agencies are using digital channels to communicate with citizens about challenges related to service delivery in their communities. The Ekurhuleni Metropolitan Municipality and City of Johannesburg (COJ) unveiled e-service solutions to promote citizenry communication and simplify cumbersome municipal operations.

Table 5-2 demonstrates applications that can be useful to a Municipalities' ICT environment.

Table 5-2: Municipal's entities requirements for Applications

Imperative	Operational Requirements	ICT Environment	Clusters Impacted
Affordability	Public sector entities require ICT costs to be low and are focused on value for money. The benefits received from the ICT environment should outweigh the costs. Costs of ownership and operating costs should be low in order to utilise taxpayers' money efficiently in transforming it into tangible outcomes for society.	The cost of ownership of particular ICT software and hardware needs to be as low as possible. This includes the initial purchase price, annual license fees and the costs associated with upgrades and maintenance.	Applications Hardware Networks

Agility	The ICT systems should be able to adapt to changes in political power, restructuring possibilities and changes in the economy. ICT should also be able to adapt to easier methods of interactions with the public.	The hardware and applications need to facilitate various systems since a public sector entity is diverse in its trade and has various stakeholders. ICT should be easy to upgrade and maintain the system	Applications Hardware
Ease of use	ICT technology should be easy to use for all users. A complex system is not desirable as it could lead to idle time, mistakes and the appointment of highly skilled staff. Decisions are made based on information captured, and therefore it is important to limit errors. The entities also want to limit the expenditure of ICT training required by complex systems.	The user interface should generate an experience for users that is not demoralising. The response rate and the content should encourage users to finalise tasks quickly and effectively. The business process should be logical, prompting for the next procedural step, require the successful completion of a step before the user can move to the next steps	Applications
Reliability	Systems need to function as intended at all times, thereby being available, effective and efficient.	The systems should be of a function of reliable quality to avoid malfunctioning. The systems should also be able to adjust to unexpected changes with minimal damage. A detailed contingency plan should be in place. A continual monitoring system that monitors the availability of systems	Applications Hardware Networks
Security	Unauthorised access to the personal data of citizens should be prevented.	Data must be kept in a valid, accurate and complete manner.	Applications Hardware Networks

		Appropriate firewalls, anti-virus programs and facilitation of administrators' rights should be in place	
Self-Service	Entities want citizens to be able to perform certain tasks directly and quickly themselves.	Online functionality should be developed and activated. User-friendly interfaces should be used to eliminate errors. A help function should be available and users should be guided step-by-step in a logical manner.	Applications

5.3.7 ICT governance

ICT g has been described as the effective and efficient management of ICT resources and processes to facilitate the achievement of municipal goals and objectives. The ICT Governance Institute describes ICT governance as “the responsibility of the board of directors and executive management” (Mohokare Local Government, 2017).

The view that ICT should be governed and managed at all levels within a given municipality structure is supported by internationally accepted good practice and standards. These practices and standards are defined in the King III Code of Good Governance, ISO 38500 Standard for the Corporate Governance of ICT and other best practice ICT Process Frameworks.

Translated into a municipal operating environment the corporate governance of ICT places a particular responsibility on the Council and Management within a municipality to ensure that the decision-making process for ICT related investments and the operational efficiencies of the municipality's ICT environments remain transparent and are upheld. This accountability enables the municipality to align the delivery of ICT services with the municipality's Integrated Development Plans and strategic goals.

According to Clara *et al.* (2018:222) the diversity of national ICT governance objectives and regulatory frameworks, good practices for ICT governance generate criteria which constitute a reference to assess government ICT initiatives in terms of economy, effectiveness, and efficiency.

These practices are generally related to stable auditing criteria in the government sector. By being related to the idea of using the audit process as a control, means that the concept of government comprises the mechanism of leadership, strategy, and control put in place to evaluate, direct and monitor the performance of management towards the conclusion of stakeholders' goals and their interests. The implementation of ICT governance principles is considered the preferred method to ensure effective, efficient, secure and acceptable use of ICT within municipalities.

ICT governance requires that certain building blocks should be in place to ensure that the municipalities strategic objectives can be met and that services can be delivered efficiently to the residents.

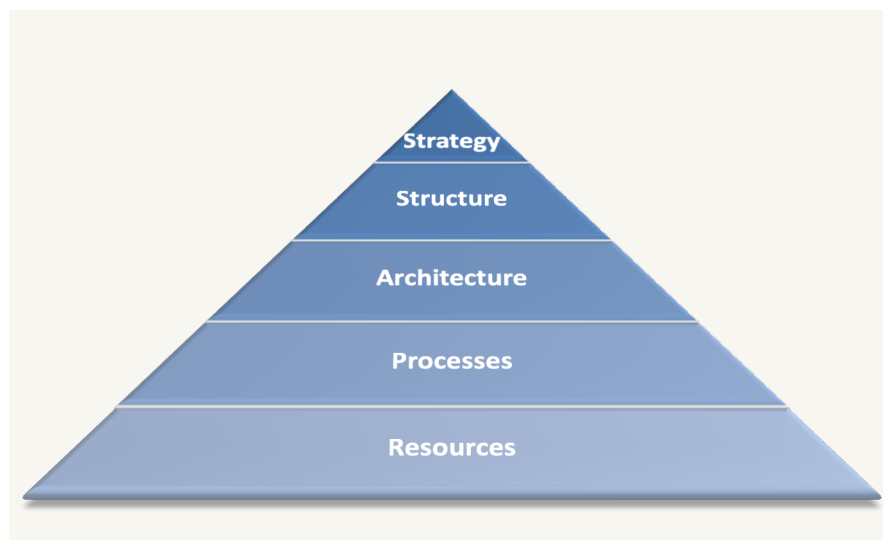


Figure 5-1: Unknown source

Figure 5-1 shows the building blocks that are required to implement an effective ICT strategy within a municipality. The building blocks contains the services that the municipality will offer, how the architecture required to support the business together with the associated processes. These components will ensure that the municipality is able to acquire the correct technologies and people who will ensure the successful implementation of an IT strategy.

The principles in Table 5-3 have been adopted in the Public Service Corporate ICT Governance Policy Framework (PSCICTGPF) which have been adapted for municipalities.

Table 5-3: ICT Governance Policy Framework

Principle 1: Political Mandate	• The Corporate Governance of ICT must enable the municipality's political mandate. • The Executive Authority must ensure that the Corporate Governance of ICT achieves the political mandate of the municipality
Principle 2: Strategic Mandate	• The Corporate Governance of ICT must enable the municipality's strategic mandate • The Accounting Officer must ensure that the Corporate Governance of ICT assists in achieving the municipality's strategic plan
Principle 3: Corporate Governance of ICT	• The Accounting Officer is responsible for the Corporate Governance of ICT • The Accounting Officer must create an enabling environment in respect to the Corporate Governance of ICT within the applicable legislative and regulatory landscape and information security context.
Principle 4: ICT Strategic Alignment	• The Executive Management must ensure that ICT service delivery is aligned with the municipality's strategic goals and that the municipality accounts for current and future capabilities • It must ensure that ICT is fit for purpose at the current service levels and quality for both current and future municipal needs.
Principle 5: Significant ICT Expenditure	• Executive Management must monitor and evaluate major ICT expenditure, ensure that the ICT expenditure is made from valid municipal business

	enabling reasons and monitor and manage the benefits, opportunities, costs and risks resulting from this expenditure, while ensuring that information assets are adequately managed
Principle 6: Risk Management and Assurance	• Executive Management must ensure that ICT risks are managed within the municipal risk management practice • Also, ensure that the ICT function is audited as part of the municipal audit plan
Principle 7: Organisational behaviour	• Executive Management must ensure that ICT service delivery is sensitive to organisational behaviour/culture • Executive Management must ensure that the use of ICT demonstrates the understanding of and respect for the organisational behaviour / culture

If ICT-enabled development interventions are to contribute to more inclusive, participatory and decentralised governance in Africa, they will have to be custom-tailored to the needs and abilities of those population groups that they seek to empower, which is the typically marginalised ones from the political participation (Breuer & Groshek, 2017:351).

According to Misuraca (2007:10) governance supported by the development of ICTs can have more powerful information transmission, stimulate debate and participation and, at the same time, the establishment of information systems and knowledge management tools can facilitate governmental processes.

It should, however, be underlined that when discussing the integration of ICTs in administration, the focus should be in the promotion of governance using ICTs as a tool, rather than the ICTs being an end in themselves.

5.3.8 ICT Strategy

Several notable policy documents regarding the Digital Divide have been developed in South Africa, including the 2016 National Integrated ICT Policy White Paper. This national ICT policy subscribes to the idea that the deployment of ICT facilitated e-centres contributes to addressing persistent inequality in the country by improving the quality of lives through accessing the benefits of, and participating in, the digital society.

Such lofty aims assume that digital transformation can enhance the efficiency of service delivery, ensure impartial access to public services by all, and improve citizens' participation in public policy-making; enhance stakeholder engagement to afford South African citizens the opportunity to access a wide range of information.

On a more practical level, the ICT policy recommends the introduction of ICT facilitated e-centres that can assist the government to address divides in society between those with resources and capabilities, and those without who are marginalised (Kassongo *et al.*, 2018:1).

According to Leibbrandt and Botha (2014:1070) developing a framework that involves strategy contributes to a better understanding of enablers that may have an effect on the ability of municipalities to execute their strategies. Such frameworks for strategy execution suggest important insights for managers and researchers and create the opportunity for future research.

Alizadeh (2017:36) argues that the first generation of digital strategies were produced for businesses of all types and sizes over 20 years ago. The idea back then was that businesses were pushed to realise that information technology had reached the mainstream, so e-business or e-commerce was everyone's business in the post-industrial new economy.

This was then followed by an influx of national digital strategies, prepared in both the developed and developing countries, in order to take advantage of the fast-growing, technology-based economy. It is often argued that national strategies were needed for digitally-enabled development in the new techno-economic paradigm.

5.3.9 Formulation of the framework

The formulation of the research framework is based on the research questions that have been identified in Chapter one after being formulated from the primary, secondary and empirical objectives. The research questions were outlined as follows:

- What role does the ICT department play within that municipality and how it compares with other similar municipalities?
- Which are the required levels of skills and education as well as the most appropriate municipality structure?
- What are the required/most suitable types of software, hardware and applications?
- Which legislative requirements or governance is in place to address the secure computerised environment?
- What strategies can be put in place to deal with challenges posed by a computerised environment?

The grouping from the questionnaire (Appendix A) was structured as follows.

- **Questions 4, 5, 6** – Free downloads without permission
- **Questions 9, 10** – Use of chatrooms
- **Questions 21, 22, 25** – Cybersecurity policies, procedures and standards
- **Questions 23, 24** – Protection of company information shared with 3rd parties
- **Questions 26, 27, 28** – Cybersecurity awareness (organisational)
- **Questions 30, 31** – Vulnerability scanning and assessment
- **Questions 33, 34, 35, 39** – Encryption and Protection
- **Questions 36, 37** – Cyber-attacks response processes
- **Questions 29, 38** – System access security
- **Questions 43, 45** – Business buy-in and ROI
- **Questions 47, 51** – Skills and a secure computer environment

To develop our framework we then match all our questions groupings from our questionnaire against the research objectives which we have listed above. Each of the research questions are tied to at least one or more of the questions groupings from the questionnaire. The questionnaire is attached as Appendix A.

Table 5-4: Research questions and groupings

Grouping	Questions	RESEARCH OBJECTIVES						
		ICT Departmental Role	Level / Type Skills	Software	Hardware	Applications	IT Governance	IT Strategy
Free- Downloads	4,5 & 6						X	
Chat - Rooms	9 & 10					X		
Cyber Security	21,22 & 25						X	
Information Protection	23 & 24	X						
Cyber Security Awareness	26, 27 & 28	X						
Vulnerability	30 & 31			X				
Encryption and Protection	33,34,35 & 39				X			
Cyber Attack Responses	36 & 37						X	
Secure Access	29 & 38							
Business buy-in and ROI	43 & 45							X
Capacity/Skill and secure environment	47 & 51		X					

5.4 THE MANAGERIAL FRAMEWORK

From the matching of the questions grouping and research objectives in the previous section (depicted as Table 5-4) the final framework is produced for a secure computerised environment in a metropolitan municipality. This framework is depicted below as a managerial framework.



Figure 5-2: The Managerial Framework

The managerial framework was developed using the research questions identified in Chapter 1 together with the questionnaire groupings from Chapter 4. The framework demonstrates how the research questions were responded to through the different areas of the questionnaire and how this would inform the recommendations that would ensure that the objectives of the study have been met.

The inner circle of the framework represents the research questions, while the next layer is the questionnaire groupings with the outermost layer being the detailed questions from the questionnaire.

Mean is the measure of central tendency that is simply the average score. To calculate the mean, all the scores were added up and then divided by the total number of scores.

Cronbach's alpha is used to measure the internal reliability or consistency of the questionnaire. The guideline value is 0.7, but 0.5 can be used although its interpretation should be handled with caution.

The Cronbach alpha values for all the grouped questions on the questionnaire are between 0.633 and 0.89. The lowest Cronbach is 0.633 for Information Protection, and the highest one is 0.89 for Free Downloads. These constructs are considered reliable as all of them are above the guideline value of at least 0.5.

5.5 CONCLUSIONS

The aim of Chapter 5 was the development of a framework for a secure computerised environment in a metropolitan municipality. The chapter began with a literature review on the theoretical framework and then began a discussion on each of the research objectives identified in Chapter 1. The question groupings from the questionnaire as indicated in Chapter 4 were matched against the research objectives in the formulation of the framework.

The chapter ends with a representation of a managerial framework which is the result of matching the research objectives against the question groupings from the questionnaire. A brief explanation of the managerial framework is provided and an overview of the mean and Cronbach alpha are provided as they are also depicted on the managerial framework.

Gabriels and Horn (2014:24) argue that “the growing gap in the provision of advanced ICTs should be of concern”. The gap for advanced ICT is growing at the same time as other determinants of poverty, such as access to education and other social services are narrowing. Weak ICT infrastructure will compromise competitiveness and in turn, constrain export-led development programmes. In addition, if new ICT expansion is limited to those who can afford it, it will contribute to expanding inequality along racial and gender lines. They further establish four levels of digital poverty.

- **Extremely digitally poor people** – people with no or very little access to new ICTs, that is, only access to radio and TV.
- **Digitally poor people** – defined as people with access to radio and TV as well as to voice telephony (either mobile, fixed or both).
- **Connected people** – people with access to the internet and email and who have access to computers.
- **Digitally wealthy people** – people who have full access to high-speed internet and/or are able to interact digitally to access e-government resources, on-line business services as well as creating their own content.

Other than the arrival of new political parties (48 in the South African government’s national elections) which were held 8 May 2019, there are significant changes in the political, social and communications platforms. Any demonstrations or group of people coming together in the form of strikes, affinity groups and trade unions, have made technology platforms (in particular social media) not only as a means for them to communicate but locate it at the centre of their preparations and planning activities.

Participation is a crucial problem in the process of introducing and promoting the use of ICTs for community development. The proper mechanism should be initiated with communities even though the biggest challenge is around finding ways to involve large segments of the population even when they are aware of the potential benefits and usefulness for ICTs. It is, therefore, most critical to understand better the attitudes of the communities towards changes, in order to identify the factors that underlie the adoption of ICTs by poor communities (Misuraca, 2007:266).

The next chapter focus on the recommendations and provides a summary of the research study results. Limitations to the study and any potential research are also identified.

CHAPTER 6: RECOMMENDATIONS AND CONCLUSIONS

6.1 INTRODUCTION

The aim of the chapter is to present the conclusions drawn from the statistical analysis of the questionnaire in Chapter 4 and be able to make recommendations. From Chapter 1, one of the study, the primary, secondary and empirical objectives were identified. All of these stated objectives resulted in the formulation of the research question.

Chapter 6 looks at how the results of the study have been able to assist in meeting the primary and secondary objectives. Once the objectives have been met, the study will provide us with a guide on the development of a framework for a secure computerised environment in a municipality.

Limitations of the research study are identified and a summary of the study results is provided, which then becomes the basis of the recommendations. The research provides indications for future research.

In accordance with the intensive use of information and communication technologies, maintaining information security has become a necessity. Attacks in cyber platforms and information loss probability force institutions to invest in information security processes.

Although the concept of information security seems to require technology-based precautions more often than not, the role of humans in this process has become more critical over time. When considered from an institutional point of view, it is seen that there are human-based errors in most of the cases that resulted in information loss. Therefore, the development of methods that force the human factor to behave in compliance with information security policies has been pursued (Kaymaz, 2020:1).

6.2 PRIMARY AND SECONDARY OBJECTIVES

The primary objective of the research was to develop a managerial framework for a secure computing environment in a metropolitan municipality. In response to all the research objectives, certain key drivers were identified to ensure that a robust managerial framework is developed to ensure a customer-centric ICT platform that is secured in the metropolitan municipality of the research study.

6.2.1 Primary objectives

The primary objective of the research study is to provide a managerial framework for a secure computerised environment in a municipality.

6.2.2 Secondary objectives

Throughout the study, the researcher has been able to identify the following secondary objectives that will provide further information on the development of the framework:

- ICT department role in the municipality
- Type and level of skills required
- A governance framework to be applied

6.2.3 Empirical objectives

The combination of the primary and secondary objectives resulted in the formation of the following empirical objectives:

- To provide input through research on how a municipality can ensure that its computerised environment is secured.
- To provide an overview of the best practice levels required for a secure computerised environment in the workplace.

6.2.4 Research questions

From all of the objectives stated above, the following research questions were formulated for the purpose of this study.

- What role does the ICT department play within that municipality and how it compares with other similar municipality?
- Which are the required levels of skills and education as well as the most appropriate municipality structure?
- What are the required/most suitable types of software, hardware and applications?
- Which legislative requirements or governance is in place to address the secure computerised environment?
- What strategies can be put in place to deal with challenges posed by a computerised environment?

This research study has been done to make a contribution to research and also provide guidelines on a framework for a secured computerised environment.

The research questions were addressed first through the literature review in Chapter 2, where the study identified major concepts in the ICT environment and also looked at what other countries on the continent and the rest of the world are doing. Furthermore, through the research instrument, the researcher was able to obtain responses from the respondents which provided statistical guidance on the current status within the City of Johannesburg.

The research study provided an overview of each of the research objectives and how each can contribute to a secure environment at the beginning of Chapter 5. The questions in the data collection research instrument were grouped together and combined with the research objectives in order to develop a managerial framework for a computerised environment in the CoJ metropolitan municipality and therefore making sure that the research study has been able to address the primary, secondary and empirical objectives through formulated research questions.

6.3 LIMITATIONS OF THE STUDY

ICT officials within the different entities in CoJ do not have a standard way of delivering their services to both internal and external customers. ICT officials within the CoJ is made up of permanent employees (both junior and senior) of the city, and consultants that are obtained through projects or services that they provide to the city. Through the establishment of the CIO Forum, the City is making strides in adopting a consolidated approach in relation to its ICT Strategy.

Limitations of the research study was the participation of the independent service providers or contractors that are in the employ of CoJ ICT environment. These independent service providers or contractors are experts that would be sourced when specialised skills that are not available within the city are required, e.g. the security experts that were brought in when the ICT environment of CoJ was hacked in November 2019. Some of these contractors and service providers performs key role in the ICT space within CoJ, in some cases these are critical outsourced services that are provided from remote locations and activated as and when they are needed.

Even though this may have resulted in a smaller sample size the lack of engagement on some of these ICT independent service providers or contractors may have an impact on the findings on some of the research questions that are posed in the research study. Given that some of the CoJ officials depends on these ICT experts for their daily functions, it is not anticipated that there would be a significant difference in how the managerial framework was developed.

For the research study, the researcher was one of the CIO forum members in CoJ and was able to identify other senior managers within the city to participate in the study. The data that was collected on experience and qualifications through the data collection instruments from the participants suggests that the contributions of the participants added great value to the research study. These senior managers were identified by the members of the CIO forum and additional questionnaires were distributed specifically to them to complete and provide their inputs in the research study.

Another limitation of the study is that most ICT officials do not fully understand their daily roles in the overall governance of the municipality, particularly on matters relating to risk management and audits.

ICT officials are scattered through the different offices within the entire City of Johannesburg and the task of distributing the questionnaires, following up on the completion as well requesting additional information proved to be a difficult task. The research study was also limited based on the information obtained through secondary data such as textbooks, the Internet, journal entries and other relevant scholar databases. These secondary data were accessed through the NWU library staff members and the different searches that are available on the website of the university's library services website.

6.4 SUMMARY OF THE STUDY RESULTS

The study has been able to address the formulated research questions that have been identified in Chapter 1. These objectives gave rise to the research objectives which identified critical aspects that would need to be addressed within the questionnaire.

The following areas, which resulted from the statistical analysis on the mean, standard deviation and Cronbach's alpha grouping of the questions in the Chapter 4, need to be addressed to ensure a sound framework for a computerised environment that can be implemented:

- Free downloads without permission
- Use of chatrooms
- Cybersecurity policies, procedures and standards
- Protection of company information shared with 3rd parties
- Cybersecurity awareness (organisational)
- Vulnerability scanning and assessments
- Encryption and protection
- Cyber-attacks response processes
- System access security
- Business buy-in and ROI
- Skills and a secure computer environment

The culture of a dedicated and efficient public service is one that is required in the municipality. Dedicated and qualified resources, such as cyber security experts, internal hackers and IT auditors should be appointed in all the ICT departments for the entities of the CoJ municipality and there should be a clear distinction between politics and administration. The research aimed at also determining the role that an ICT department should take in the business and the required type and level of skill that will enable such a secure ICT environment.

The required software, hardware, and ICT platforms that will ensure a competitive edge for the business without compromising the informational assets of the municipality were studied closely. It is often heard how many municipalities are unable to spend their CAPEX budgets which are aimed at improving or building the required infrastructure to supports their technology platforms and systems.

In order to produce a cultural shift in the research community, the change process needs to extend to traditional university training programmes in which research methodology and statistics are taught to future generations of graduate students (Kratochwill & Levin, 2014:234).

The research study looked at the personal awareness of each user and their experiences with regard to the usage of a computer and the internet at large. The study then delved deeper into the area of audit, which is critical for the CoJ ICT departments as the Auditor-General conducts annual audits looking at people, processes and technologies that are in place.

The general responses indicate that even though the participants are aware of both internal and external audits conducted in their workplace, there is not enough awareness in terms of how they could each contribute towards clean audits in their ICT department.

Management must ensure that their ICT strategies are approved and implemented in their municipality. The implementation of such strategies requires investments in both financial systems and human capital to enable a secure computerised environment.

Businesses should not regard ICT departments as just another support department. ICT departments should always be viewed as a strategic partner which enables the business to leverage on the best available technologies in order to attain a competitive edge and as a result increase profits and/or the quality of the service offerings that it provides.

ICT management in the CoJ municipality should further ensure that all activities that are performed by their ICT department in support of their ICT strategies are geared towards minimising risks and achieving clean audits both internally and externally.

According to Gecer and Benzer (2019:64) the basic reason behind scientific studies is to collect valid and reliable information. The primary method of gathering scientific information is the process of measurement. Valid and reliable measurement instruments are some of the cornerstones of scientific research. In other words, the process of measurement is often utilised to measure different abilities, perceptions and attitudes of individuals in research studies; to make certain decisions based on them.

6.5 RECOMMENDATIONS

The recommendations of the research emanate from the answers in response to the grouped questions from the questionnaire and the research objectives identified in Chapter 1. The combination of the grouped questions and the research objectives were used in the development of the managerial framework in Chapter 5.

The recommendations listed below are based on the managerial framework developed in Chapter 5 which gets into the analysis of the questionnaire and the critical elements that needs to be addressed in order to ensure a secure computerised environment.

The following list of recommendations should be implemented by all the ICT department of the CoJ metropolitan municipality to ensure a secure computerised environment in the workplace:

- There should be a formal process in place to respond to any Cyber Attack threats.
- A resourced and skilled computer response incident team should be a part of the ICT department.
- Internal and external audits must be performed in the ICT environment at least once a year.
- Cyber security education and awareness should consistently take place in the entire municipality.
- All the ICT departments within the CoJ municipality should ensure that there are skilled security specialist within their teams.
- All cyber security processes that are implemented should be compliant to all applicable laws, policies and standards.
- All ICT policies within the municipality must be documented and approved through the applicable process of the municipality with their review periods/updates also indicated.
- All company devices should be encrypted.
- Mobile devices should have functionality that enables remote abilities.
- ICT devices should all be accessed by independent usernames and passwords for all users of the systems.
- Monitoring tools should be implemented on all the devices within the ICT infrastructure.

- ICT infrastructure should be enabled with firewalls for all the devices within the environment.
- All CoJ employees should not be allowed/permitted to download any programs, videos and music without permission.
- Any remote access in the environment should be done using a two-factor authentication.
- All systems, platforms, databases and applications within the workplace, should be accessed with a username and password.
- The ICT department must have staff for their environment with the required levels of skills and expertise for roles that are to be performed in the workplace.
- There should be enough staff compliment in the ICT department to ensure that the environment is secured.
- The ICT department should not be viewed as a support department but rather a strategic partner within the operations of the entire municipality.
- The CoJ municipality should derive added business value and positive returns in the ICT investments that it has made to all the entities' ICT departments.
- The returns and any added business value should provide the municipality with a competitive edge in its provision of services.
- Vulnerability scanning software should be in place in the environment and associated remedial actions, such as ensuring that scans are scheduled and performed and that any recommendations from the scans are followed and implemented.
- A risk register for the ICT department should be maintained and updated at all times to ensure that sound controls are in place within the environment.
- All CoJ employees should be encouraged to make use of secured instant message programs and chat rooms only for work related purposes and such restrictions should be communicated and enforced.

6.6 INDICATIONS FOR FUTURE RESEARCH

It is recommended that future research be expanded to the other metropolitan municipalities in Gauteng (City of Tshwane and Ekurhuleni). The expanded study will provide guidance on how other municipalities in the other provinces within the country have structured their computerised environments in order to meet their service delivery offerings to their citizens.

Further research can be done on the other developing (Brazil and China) and developed countries (USA and Germany) on how they offer services to their citizens making use of the technology environment that is available to them.

6.7 CONCLUSION

This chapter has provided a summary of the primary, secondary and empirical objectives which formulated the research questions, the research design, interpretation of the study and its limitations. A number of the research recommendations has been provided including indications for future research.

This research study has constructed a list of ICT guidelines that have been confirmed as being the most important to the development of a managerial framework in a computerised environment of a metropolitan municipality. These guidelines were supported through the questions from the questionnaire that were grouped together in order to respond to the research questions of the study.

The study also seeks to contribute to the body of knowledge on ITC for a secure computerised environment in a metropolitan municipality in the following four ways.

- By providing empirical evidence on the current state of a computerised environment in CoJ obtained from the perspective of the participants in the study.
- By making use of literature review to provide an understanding of the major concepts in ICT security.
- By proposing a set of guidelines that serves as a control and mitigate against risk in ensuring that a computerised environment in the metropolitan municipality.
- By providing the entities' CIOs with a series of recommendations that are associated with the managerial framework that have been proposed in the research study.

Municipal entities' CIOs or any other ICT officials should give consideration to the suggested recommendations in the research study and furthermore ensure that they are able to obtain buy-in from their respective CEOs, boards and their political leadership.

REFERENCE LIST

- Abi Sen, A. A. & Basahel, A. M. 2019. A comparative study between security and privacy. Proceedings of the 13th IndiaCom.
- Aderinoye, R. 2008. Literacy and communication technologies: distance education strategies for literacy delivery. *International Review of Education*, 54:605–626.
- Adonis, V.A. 2018. Performance management system for strategy implementation in local government. *Journal of Public Administration*, 53(2):261–275.
- Adom, D., Hussein, E.K. & Agyem, J. 2018. Theoretical and conceptual framework: mandatory ingredients of a quality research. *International Journal of Scientific Research*, 7(1):438–441.
- Agee, J. 2009. Developing qualitative research questions: a reflective process. *International Journal of Qualitative Studies in Education*, 22(4):431–447.
- Ahmad, J., Li, S., Thavot, R. & Mattavelli, M. 2013. Signal processing: *Image Communication*, 28:1315–1334.
- Alali, M., Alogren, A., Hassan, M.M., Rassan, I.A.L. & Bhuiyan, M.Z.A. 2018. Improving risk assessment model of cyber security using fuzzy logic inference system. *Science Direct, Computers & Security*, 74:323–339.
- Alasuutari, P., Bickman, L. & Brannen, J. 2009. The SAGE handbook of social research methods. Paperback edition. SAGE Publications, UK.
- Ali, Z. & Bhashkar, S.B. 2016. Basic statistical tools in research and data analysis. *Indian Journal of Anaesthesia*, 60:662–669.
- Alizadeh, T. 2017. Urban digital strategies: Planning in the face of Information Technology. *Journal of Urban Technology*, 24(2):35–49.
- Almasizadeh, J. & Azgomi, M.A. 2016. Mean privacy: A metric for security of computer systems. *Science Direct, Computer Communications*, 52:47–59.

- Antonius, R. 2013. Interpreting quantitative data with IBM SPSS Statistics. 2nd ed. Sage Publications, UK.
- Aoto, P.C., Fenwick, R.B., Kroon, G.J.A. & Wright, P.E. 2014. Accurate scoring of non-uniform sampling schemes for quantitative NMR. *Journal of Magnetic Resonance*, 246:31–35.
- Arora, N. 2017. Qualitative research in management: methods and experiences. *South Asian Journal of Management*, 24(1):196–199.
- Bader, F. 2014. Methods for quantitative macro-comparative research. *Swiss Journal of Sociology*, 40(3):535–538.
- Baillie, L. 2013. Enhancing observational data in qualitative research. *Nurse Researcher*, 20(5):4–5.
- Bauer, S., Bernroider, E.W.N. & Chudzikowski, K. 2017. Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Science Direct, Computers and Security*, 68:145–159.
- Belanger, F., Collignon, S., Enget, K. & Negangard, E. 2017. Determinants of early conformance with information security policies. *Information and Management*, 54:887–901.
- Bertucio, B. 2017. The Cartesian heritage of Bloom's taxonomy. *Scientific Philosophical Education*, 36:477–497.
- Braekman, E., Barete, F., Charafeddine, R., Demarest, S., Drieskens, S., Gisle, L., Molenberghs, G., Tafforeau, J., Van Der Heyden & Van Hal, G. 2018. Measurement agreement of the self-administered questionnaire of the Belgian health interview survey: paper and pencil versus web-based mode. *PLOS one*, 1–13.
- Breuer, A. & Groshek, J. 2017. Assessing the potential of ICTs for participatory development in Sub-Saharan Africa with evidence from urban Togo. *International Journal of Political and Cultural Society*, 30:349–368.

- Brown, N.M.K., Lui, C. Robinson, P.C. & Boyle, F.M. 2015. Supportive care needs and preferences of lung cancer patients: a semi-structured qualitative interview study. *Support Care Cancer*, 23:1533–1539.
- Burnap, P., French, R., Turner, F. & Jones, K. 2018. Malware classification using self-organising feature maps and machine activity data. *Science Direct, Computers and Security*, 73:399–410.
- Buys, R. 2000. Love Hurts: Computer, network and e-mail security. *De Rebus*, 390:33.
- Campbell, J.L., Quincy, C., Osserman, J. & Pedersen, O.K. 2013. Coding in-depth semi-structured interviews: problems of unitization and inter-coder reliability and agreement. *American Sociological Association*, 1–24.
- Carslaw, D. 2014. Modern tools for air quality data analysis—openair. *The Clean Air Journal*, 24(2):4–5.
- Chen, L. & Tao, L. 2012. Web security using portable virtual labs. *Journal of Educational Technology and Society*, 15(4):39–46.
- Chesterman, S. 2018. How public is Public International Law? Toward a typology of NGOs and Civil Society Actors. *The Global Forum*, 24:159–168.
- Chilisa, B. & Kawulich, B. 2012. Selecting a research approach: Paradigm, methodology and methods. (In Wagner, C., Kawulich, B. & Garner, M., eds. *Doing social research: A global context*. New York: McGraw Hill. p. 51–61).
- Chisango, G. & Lesame, C. 2017. Challenges of information and communication technology policy implementation in rural South Africa. *Communitas*, 22:48–61.
- Chowdhury, M.F. 2014. Interpretivism in aiding our understanding of the contemporary social world. *Open Journal of Philosophy*, 4:432–438.
- Clara, A.M.C., Canedo, E.D. & de Sousa Junior, R.T. 2018. A synthesis of common guidelines for regulatory compliance verification in the context of ICT governance audits. *Information Polity*, 23(2):221–237.

- Cobb, C., Sudar, S., Reiter, N., Anderson, R., Roesner, F. & Khono, T. 2018. Computer Security for data collection technologies. *Science Direct: Development Engineering*, 3: 1–11.
- Cordery, C., Belal, A.R. & Thomson, I. 2019. NGO accounting and accountability: past, present and future. *Accounting Forum*, 43(1): 1-15,
- Coleman, A. 2014. Information and Communication Technology (ICT) framework for African traditional governance. *Indilinga African Journal of Indigenous Knowledge Systems*, 13:177–187.
- Cornell, R.M., Johnson, B.C. & Schwartz, Jr. W.C. 2013. Enhancing student experimental learning with structured interviews. *Journal of Education for Business*, 88:136–146.
- Cronje, F. 2014. Research design and research paradigm should be led by research questions: a mixed methods approach. <http://iiespace.iie.ac.za/handle/11622/48> Date of access: 31 Mar. 2020.
- De Angelis, G. 2015. The foundation of a critical social theory: Lessons from the Positivusstreit. *Journal of Classical Sociology*, 15(2):170–184.
- de Bruin, B. & Floridi, L. 2017. The Ethics of Cloud Computing. *Science Engineering Ethics*, 23: 21–39.
- Dana, J., Dawes, R. & Peterson, N. 2013. Belief in the unstructured interview: The persistent of an illusion. *Judgement and Decision Making*, 8(5):512–520.
- Dang-Pham, D., Pittayachawan, S. & Bruno, V. 2017. Investigation into the formation of information security influence: Network analysis of an emerging organisation. *Science Direct, Computers and Security* 70:111–123.
- Dammak, A. 2015. Research Paradigms: Methodologies and compatible methods. *The Academic Journal of St. Clements Education Group*, 6(2):1–14.
- Davies, M. & Hughes, N. 2015. Doing a successful research project: using qualitative and quantitative methods. *Social Work Education*, 34(2):244–248.

- Dowling, R., Lloyd, K. & Suchet-Pearson, S. 2016. Qualitative methods 1: Enriching the interview. *Progress in Human Geography*, 40(5):679–686.
- Duffy, T. 2011. Helping local governments improve cyber security. *Public management, Tech Touch Security*, p. 21.
- Dutwin, D. & Buskirk, T.D. 2017. Apples to oranges or gala versus golden delicious? comparing data quality of non-probability internet samples to low response rate probability samples. *Public Opinion Quarterly*, 81:213–249.
- Dysart, J. 2013. Lock it up: Lax data security can cost you clients. *American Bar Association*, 99(4):31.
- Egelman, S. & Peer, E. 2015, September. The myth of the average user: Improving privacy and security systems through individualization. In *Proceedings of the 2015 New Security Paradigms Workshop* (pp. 16-28).
- El-Latif, A.A., El-Atty, B., Hossain, M.S., Elmougy, S. & Ghoneim, A. 2017. Secure quantum steganography protocol for fog Cloud Internet of Things. *IEEE Access*, 6:10332–10340.
- Elliot, M.N., Mccaffrey, D., Perlman, J., Marshall, G.N. & Hambarsoomians, K. 2009. Use of expert ratings as sampling strata for a more cost-effective probability sample of a rare population. *Public Opinion Quarterly*, 73(1):56–73.
- Etchegaray, J.M. & Fischer, W.G. 2011. Understanding evidence-based research methods: pilot testing surveys. *Health Environments Research and Design Journal*, 4(4):143–147.
- Fassinger, R. & Morrow, S.L. 2013. Towards best practices in quantitative, qualitative, and mixed-method research: a social justice perspective. *Journal for Social Action in Counselling and Psychology*, 5(2):69–83.
- Field, A. 2013. *Discovering Statistics using IBM SPSS Statistics*. SAGE Publishers, UK.
- Flick, U. 2011. *Introducing research methodology: a beginner's guide to doing a research project*. SAGE Publishers, UK.

Fonseca, M. 2013. Most common reasons for journal rejections. www.editage.com/insights/most-common-reasons-for-journal-rejections. Date accessed: 9 June 2017.

Food Review 2018. Breaches in Cyber security. www.cisco.com. Date of Access: 20 April 2018.

Fowler, F.J. 2009. Survey research methods: applied social research methods series. 4th ed. SAGE Publications, UK.

Frankson, L. 2016. Municipalities get smart: Technology. *IMIESA*, 41(2):77–78.

Gabriels, H. & Horn, A. 2014. The relationship between access to Information and Communications Technology (ICT) and poverty in South Africa. *Africanus*, 44(1):21–33.

Gallagher, J. 2016. Interviews as catastrophic encounters: an object relations methodology for IR research. *International Studies Perspectives*, 17:445–461.

Gantt, E.E., Lindstrom, J.P. & Williams, R. N. 2016. The general theory and the specificity of social behaviour: Contrasting experimental and hermeneutic social science. *Journal for the Theory of Social Behaviour*, 47(2):130–153.

Gay, C.H. & McCoy, F. 2012. Career Outlook: Spotlight on Information Security. *Hispanic Engineer and Information Technology*, 27(1):44, 46–56.

Gay, G.H. 2011. Vulnerabilities in cyber security mean opportunities too. *US Black Engineer and Information Technology*, 35(4):68–69.

Gcukamana, M. 2009. Computer security gets its own response team. *CSIR Science Scope*, (3):46 -47.

Gecer, Y. & Benzer, R. 2019. Scale development/Adaptation studies conducted with the scope of cyber threats and information security issues. *Internal Journal of Information Security Science*, 9(1):64–75.

Geier, J. T. 2010. Designing and Deploying 802.11n Wireless Networks. Indianapolis Ind: Cisco Press.

- Geuens, M. & De Pelsmacker, P. 2017. Planning and conducting experimental advertising research and questionnaire design. *Journal of Advertising*, 46(1):83–100.
- Gollman, D. 2011. Computer Security. 3rd ed. John Wiley and Sons: UK.
- Gomez, A., Elboj, C. & Capllonch, M. 2013. Beyond action research. the communicative methodology of research. *International Review of Qualitative Research*, 6(2):183–197.
- Graham, K.W. 2015. A dynamic capabilities view of technology adoption success: The influence of micro-politics. Mississippi State University, ProQuest Dissertations Publishing.
- Grant, C. & Osanloo, A. 2014. Understanding, selecting and integrating a theoretical framework in dissertation research: creating the blueprint for your 'house'. *Administrative Issues Journal*, 4(2):12–26.
- Gratian, M., Bandi, S., Cukier, M., Dykstra, J. & Ginther, A. 2018. Correlating human traits and cyber security behaviour intentions. *Science Direct: Computers & Security*, 73:345–358.
- Green, H. 2016. Use of theoretical and conceptual frameworks in Qualitative Research. 1- 7.
- Gupta, S. & Dham, R. 2017. Connecting quickly and Economically to the IoT. *Electronic Component News*, 61(4):16–17.
- Gurtoo, A. 2011. Research design: qualitative, quantitative, and mixed methods approaches. *Current Science*, 101(5):683–684.
- Gutzwiller, K.J. & Riffell, S.K. 2014. Rigor and transparency in statistical analyses can help to ensure valid research. *Landscape Ecology*, 29:1115–1122.
- Hadfield, M. 2012. Becoming critical again: reconnecting critical social theory with the practice of action research. *Educational Action Research*, 20(4):571–585.
- Hall, I. 2014. The promise and perils of interpretivism in Australian international relations. *Australian Journal of Public Administration*, 73(3):307–316.

- Hassan, N.K. & Mingers, J. 2018. Reinterpreting the Kuhnain Paradigm in Information Systems. *Journal of the Association for Information Systems*, 19(7):568–599.
- Hartwell, C.J. & Campion, M.A. 2016. Getting on the same page: The effect of normative feedback interventions on structured interview ratings. *Journal of Applied Psychology*, 101(6):757–778.
- Hermans, C & Schoeman, W. J. 2015. Practice-oriented research in service of designing interventions. *Acta Theologica*, 2: 26 – 44.
- Hesse-Biber, S. 2016. Qualitative or mixed methods, research inquiry approaches: some loose guidelines for publishing in sex roles. *Springer Science*, 74(1):6-9.
- Horvath, K. 2012. National numbers for transnational relations? Challenges of integrating quantitative methods into research on transnational labour market relations. *Journal of Ethnic and Racial Studies*. 35 (10) : 1741 – 1757.
- Holley, K. & Colyar, J. 2012. Under construction: how narrative elements shape qualitative research. *Theory Into Practice*, 51(2):114–121.
- Hovorka, D.S. & Lee, A.S. 2010. Reframing interpretivism and positivism as understanding and explanation: consequences for information systems research. *International Conference on Information Systems*, 188:1–13.
- Hsu, C., Lee, J. & Straub, D. 2012. Institutional influences on information systems security innovations. *Information Systems Research*, 23(3):918–939.
- Inan, F.A., Namin, A.S., Pogrund, R.L. & Jones, K.S. 2016. Internet use and Cybersecurity concerns of individuals with visual impairments. *Journal of Educational Technology & Society*, 19(1):28–40.
- Intergrated Development Plan, 2019/2020 Review. www.joburg.org.za/Documents/2019. Date of Access, 22 July 2020.
- Internet of things: Status and implications of an increasingly connected world. 2017. *GAO(U.S. Government Accountability Office) Reports* :1–3.

- Iyamu, T. 2018. A multilevel approach to big data analysis using analytic tools and actor network theory. *The South African Journal of Information Management*, 20(1):1- 9.
- Jansen, H. 2010. The Logic of Qualitative Survey Research and its Position in the Field of Social Research Methods. *Forum: Qualitative Social Research* (11)2.
- Jorgenson, D.W. & Vu, K.M. 2016. The ICT revolution, world economic growth, and policy issues. *Science Direct, Telecommunications policy*, 40:383–397.
- Joseph, M.K. & Ogra, A. 2013. ICT reforms and citizen service delivery—lessons from municipal ICT Applications. *COGIT*, 5:25–32.
- Joseph, S. & Olugbara, O. 2017. Evaluation of municipal e-government readiness using structural equation modelling technique. *The Journal for Transdisciplinary Research in Southern Africa*, 14:1–10.
- Kaboub, F. 2008. Positivist Paradigm. *Leong*, 2(2):343.
- Kaiser, G. & Smallwood, J. 2014. Towards a systems thinking approach in allocating infrastructure budgets in local government. *Journal of the South African Institution of Civil Engineering*, 56(1):93–99.
- Kaselowski, E., von Solms, B. & von Solms, R. 2010. Municipalities and information technology governance—towards a strategic planning framework. *Journal of Public Administration*, 45(2):333–342.
- Kassongo, F.R., Tucker, D.W. & Pather, S. 2018. Government facilitated access to ICT's: Adoption, use and impact on the well-being of indigent South Africans. *IST Africa Conference*, 1–10.
- Kawulich, B. & Chilisa, B. 2012. www.researchgate.net/publications/257944787. _Date Accessed: 30 May 2018.
- Kaymaz, K. 2020. The analysis of the relations among normative beliefs, self-efficacy and intention to comply within the frame of information security policies. *The Journal of Industrial Relations and Human Resource*, 22(1):1–20.

- Keightley, E., Pickering, M. & Allett, N. 2011. The self-interview: a new method in social science research. *International Journal of Social Research Methodology*, 15(6):507–521.
- Kemmis, S. 2010. What is to be done? The place of action research. *Educational action research*, 18:417–427.
- Ketefian, S. 2015. Ethical considerations in research. Focus on vulnerable groups. *Invest Educ Enferm*, 33(1):165–172.
- Kiessling, T. & Harvey, M. 2005. Strategic global human resource management research in the twenty-first century: an endorsement of the mixed-method research methodology. *International Journal of Human Resource Management*, 16(1):22–45.
- Kirkpatrick, G. 2003. Evolution or Progress? A (Critical) Defence of Habermas' Theory of Social Development. *Thesis Eleven*, 72:91–112.
- Kocher, P. 2016. Privacy and Security. Computer Security is broken: Can better hardware help fix it? *Communications of the ACM*, 59(8):22–26.
- Kratochwill, T.R. & Levin, J.R. 2014. Meta and statistical analysis of single-case intervention research data: Quantitative gifts and a wish list. *Journal of School Psychology*, 52:231–235.
- Kunyenje, G. & Chigona, W. 2019. External Actors in Forming National ICT Policy in Malawi: A Cause for Concern in Low-Income Countries? *African Journal of Information Systems*, 11(1): Article 2.
- Lach, D. 2014. Challenges of Interdisciplinary Research: Reconciling Qualitative and Quantitative Methods for Understanding Human-Landscape Systems. *Environmental Management*, 53:88–93.
- Laher, S. 2016. Ostinato rigor: establishing methodological rigour in quantitative research. *South African Journal of Psychology*, 46(3):316–327.
- Landwehr, C.E. 2001. Computer security. *International Journal of Innovation Science*, (1):3–13.
- Laurie, C. & Jensen, E.A. 2015. Doing Real Research. SAGE Publications, UK.

- Lee, C., Yim, H. B. & Seong, P. H. 2018. Development of a quantitative method for evaluating the efficacy of cyber security controls in NPPs based on intrusion tolerant concept. *Science Direct, Annals of Nuclear Energy*, 112:646–654.
- Lee, H. , Lee, D. , Moon, J. , Jung, J. , Kang, D. , Kim, H. & Won, D. 2017. An improved anonymous authentication scheme for roaming in ubiquitous networks. *PLOS ONE*, 13(3):1- 33.
- Leibbrandt, J.H. & Botha, C.J. 2014. Development of an Integrated Operating Framework for Strategy Execution in Gauteng Municipalities in South Africa. *International Business & Economics Research Journal*, 13(5):1057–1076.
- Letue, F., Martinez, M., Samson, A., Vilain, A. & Vilain, C. 2018. Statistical methodology for the analysis of repeated duration data in behavioral studies. *Journal of Speech, Language, and Hearing Research*, 61:561–582.
- Lin, Y., Durbin, J.M. & Rancer, A., S. 2016. Math Anxiety, Need for Cognition, and Learning Strategies in Quantitative Communication Research Methods Courses. *Communication Quarterly*, 64(4):390–409.
- Lombard, K. & Kloppers, M. 2015. Undergraduate student's teachers' views and experiences of a compulsory course in research methods. *South African Journal of Education*, 35(1):1–14.
- Maglaras, A.L., Kim, K., Janicke, H., Ferrag, A. M., Rallis, S., Fragkou, P., Maglaras, A. & Cruz, J.T. 2018. Cyber Security of critical infrastructures. *Science Direct, ICT Express* 4:42–45.
- Marais, C.W. 2013. Local authority security: its role and responsibility in law enforcement. *Acta Criminologica*, 16(3):124–129.
- Maree, K. & Pietersen, J. 2020. Sampling. First steps in research, 3rd edition, Pretoria, Van Schaik.
- Mawela, T., Ochara, M.N. & Twinomurinzi, H. 2017. E-Government Implementation: A Reflection on the South African Municipalities. *South African Computer Journal*, 29(1):147–171.

- McCarthy, G.A. 2016. Adolescents in second language qualitative research: managing the interview interface. *New Zealand Studies in Applied Linguistics*, 22(1):37–51.
- McDonald, A. 2015. Accurate detection of intrusion in information networks: information security. *CSIR Science Scope*, 8:46–47.
- McDougall, D.A. 2017. Is Wittgenstein Presenting a Reductio Ad Absurdum Argument in the 'Private Language' Sections of Philosophical Investigations. *The Philosophical Quarterly*, 67(267):552–570.
- Meenakshi, S., Goel, S., Singh, S.K., Sharma, R. & Gupta, P.K. 2015. External validity and non-probability sampling. *Indian Journal of Medical Research*, 141(4):487–488.
- Miller, G.P., Johnston, J., Dunn, M., Fry, C.L. & Degenhardt, L. 2010. Comparing probability sampling methods in ecstasy research: implication for the Internet as a research tool. *Substance Use and Misuse*, 45(3):437–450.
- Misucara, G.C. 2007. E-governance in Africa, from theory to action: a handbook on ICTs for local governance. Africa World Press Publications: USA.
- Mohokare Local Government. 2017. ICT Strategic Plan: 2015-2019. https://www.mohokare.gov.za/documents/policies/2017/Information%20Technology/ICT%20Strategic_2015_to_2019.pdf Date accessed: July 2019.
- Mokhele, I. & De Beer, K. J. 2007. The use of Information and Communications Technology (ICT) in e-service delivery and effective governance in South Africa. *South African ePublications*, 6(2):60 -67.
- Morley, D. 2010. Understanding of computers in a changing society. 4th ed. Cengage Learning: USA.
- Morrison, M.I. 2013. The acquisition supply chain and the security of government information technology purchases. *Public Contract Law Journal*, 42(4):749-792.
- Mulaudzi, M.C. 2016. Testing measurement invariance of the learning programme management and evaluation scale across academic achievement. *South African Journal of Human Resource Management*, 14(1):1–8.

Muller, K. 2007. A framework for assessing environmental governance structures. *Journal of Public Administration*, 42(1):18–32.

Municipal corporate governance of ICT. www.belabela.gov.za. Date of access: 12 May 2018.

Murenzi, P. & Olivier, B. 2017. E-Government Challenges faced by Selected District Municipalities in South Africa and Rwanda. *Administratio Publica*, 25(1):141–171.

Murphy, M., Hollinghurst, S. & Salisbury, C. 2018. Qualitative assessment of the primary care outcomes questionnaire: a cognitive interview study. *BMC Health Service Research*, 18(1):1–14.

Mpuru, L. 2017. Cyber security concerns in South Africa: current legislative framework. *Servamus Community-based Safety and Security Magazine*, 110:44–45.

Mzekandaba, S. 2018. SA's R&D expenditure climbs to R38bn. IT Web: <http://hdl.handle.net/20.500.11910/15124>. Date Accessed: 21 January 2020.

Naidoo, K. & Nsibirwa, Z. 2015. The information behaviour of managers in the Msunduzi Municipality's business units. *Innovations*, 51:3–21.

Nel, F. & Drevin, L. 2019. Key elements of an information security culture in organisations. *Information and Computer Security*, 27(2): 146 – 164.

Nelwamondo, F. 2010. Building a strong local information security competence and reducing SA's dependency on imported information security solutions: 49 -50.

Nwagwu, W.E. & Ibeku, S. 2016. Understanding the innovativeness of information technology products and service providers in an IT cluster in Nigeria. *South African Journal Libraries and Information Science*, 82(1):36–52.

Onwuegbuzie, A.J. 2002. Why can't we all get along? Towards a framework for unifying research paradigms. *Education*, 122(3):518–530.

Okurumeh, O.A. & Ukaoha, K.C. 2015. Information security issues surrounding use of social media networks in organisations: An appraisal. *Journal of Emerging Trends in Engineering and Applied Sciences*, 6(23):227–232.

Oxley, A. 2013. Security risks in social media technologies. Safe practices in public service applications. Chandos Publishing : UK.

Pack, J. 2019. Cybersecurity for distributed energy resources and SCADA systems. www.tdworl.com. Data Accessed : 24 July 2020.

Panneerselvam, J., Liu, L. & Antonopoulos, N. 2018. InOt-RePCoN: Forecasting user behavioural trend in large-scale cloud environments. *Science Direct, Future Generation Computer Systems*, 80:322–341.

Parent, L. 2016. The wheeling interview: mobile methods and disability. *Mobilities*, 11(4):521–532.

Park, H., Sha, M.M. & Pan, Y. 2014. Investigating validity and effectiveness of cognitive interviewing as a pretesting method for non-English questionnaires: findings from Korean Cognitive interviews. *International Journal of Social Research Methodology*, 17(6):643–658.

Park, J., Suh, Y. & Park, C. 2016. Implementation of cyber security for safety systems of nuclear facilities. *Science Direct, Progress in Nuclear Energy*, 88:88–94.

Parker, J.S. 2012. Lost in the cloud: Protecting end-user privacy in federal cloud computing contracts. *Public Contract Law Journal*, 41(2):385–409.

Patrick, H.A. 2018. Impact of leadership strategies of managers on employees in information technology organisations. *The Journal–Contemporary Management Research*, 12(1):1- 13.

Philander, K.S., Gainsbury, S.M. & Grattan, G. 2019. An assessment of the validity of the Gamblers belief questionnaire. *Addictive Behaviours*, 97:104–110.

Pillay, S. 2002. Public administration and the future: Modernising government through information technology. *Journal of Public of Administration*, 37(2) :103–121.

Ponelis, S.R. 2015. Using interpretative qualitative case studies for exploratory research in doctoral studies: a case of Information System Research in small and medium enterprise. *International Journal of Doctoral Studies*, (10):535–550.

Punch, K.F. 2014. Introduction to social research quantitative and qualitative approaches, 3rd ed. SAGE Publications, UK.

Ragaad, B.G. 2010. Information Security Management, concepts and practice. New York: CRC Press.

Rahi, S. 2017. Research design and methods: A systematic review of research paradigms, sampling issues and instruments development. *International Journal of Economics & Management Sciences*, 6(2):1–5.

Raina, K.S. 2014. Self weighing and non-probability samples. *Indian Journal of Medical Research*, 140:149–150.

Reischauer, G. 2015. Combining artefacts analysis, interview and participants observation to the study the organisational sense making of knowledge-based innovation. *Historical Social Research*, 40(3):279–298.

Rezaeibagha, F. & Mu, Y. 2018. Practical and secure telemedicine systems of user mobility. *Science Direct, Journal of Biomedical Informatics* 78:24–32.

Ribbs, G.R., Friese, S. & Mangabeira, W.C. 2002. The use of New Technology in Qualitative Research. *Introduction to 3(2) of Forum: Qualitative Social Research*.

Ryan, T.P. 2015. Sample size determination and power. *International Statistical Review*, 83(1):160–174.

Safa, N.S., Maple, C., Watson, T. & Solms, R.V. 2017. Motivation and opportunity based model to reduce information security insider threats in organisations. *Science Direct, Journal of Information Security and Applications*: 1–11.

Salau, A.O. 2017. The right of access to information and national security in the African regional human rights system. *African Human Rights Law Journal*, 17: 367-389

Salomon, D. 2006. Foundations of Computer Security. Springer-Verlag: UK. Sandberg, K.W., Gardelli, A. & Stubbs, J. 2005. The use of Information and Communication Technology (ICT) in the rehabilitation of individuals with severe functional impairments in a municipal care service system. *IOS Press*, 24:229–238.

- Sani, S.A., Yuan, D., Jin, J., Gao, L., Yu, S. & Dong, Y. Z. 2018. Cyber security framework for Internet of Things-based Energy Internet. *Science Direct, Future Generation Computer Systems*, 1–11.
- Sareen, S., Gupya, S., K. & Sood, S., K. 2017. An intelligent and secure system for predicting and preventing Zika virus outbreak using Fog Computing. *Enterprise Information System*, 11(9): 1436 – 1456.
- Scharff, R. C. 2007. On weak Postpositivism: a historical rejection of the view from nowhere. *Journal Compilation*, 38(4):510–534.
- Schatz, E. & Williams, J. 2012. Measuring gender and reproductive health in Africa using demographic and health surveys: the need for mixed-methods research. *Culture, Health and Sexuality*, 14(7):811–826.
- Scholl, H.J. & AlAwadhi, S. 2016. Creating Smart Governance: The key to radical ICT overhaul at the City of Munich. *IOS Press*, 21:21–42.
- Schurink, E. 2009. Qualitative Research Design as Tool for Trustworthy Research. *Journal of Public Administration*, 44(4.2):803 -823.
- Shamala, P., Ahmad, R., Zolait, A. & Sedek, M. 2017. Integrating information quality dimensions into information security risk management (ISRM). *Journal of information security and applications*, 36:1- 10.
- Shanthi, S., Kannan, R., J. & Shanthi, S. 2018. Efficient secure systems of data in cloud using steganography based cryptosystem. *Materials Proceedings*, 5:1967–1973.
- Siewe, F. 2016. Towards the modelling of secure pervasive computing systems: A paradigm of context-aware secure action system. *J. Parallel Distribut. Comput*, 87:121–144.
- Smith, G.S., Swanson, W.D., Chiappone, M., Miller, L.S. & Ault, S. J. 2011. Probability sampling of stony coral populations in the Florida Keys. *Enviromental Monitoring and Assessment*, 183(1-4):121–138.
- Smith, P. 2012. A Municipal Guide/Roadmap To Successful ICT Governance. *South African Local Government Association*.

Snyder, J. 2012. Careers in Information Security. *Women of Color Magazine*, 11(1):25–27.

Solomon, M.G., Kim, D. & Carrell, J. L. 2015. Fundamentals of Communications and Networking. 2nd ed. Jones & Bartlett Learning: USA.

Sorrentino, M., De Marco, M. & Depaoli, P. 2017. ICT policies, the Mediterranean tradition and the Italian diet of discontinuity. *Science Direct: Telematics and Informatics*, 34:707–716.

Steen, J., DeFillippi, R., Sydow, J., Pryke, S. & Michelfelder, I. 2018. Projects and networks: understanding resource flows and governance of temporary organisations with quantitative and qualitative research methods. *Project Management Journal*, 49(2):3–17.

Steffen, M.W., Murad, M.H., Hays, J.T., Newcomb, D.R., Molella, G.R., Cha, S. S. & Hagen, P.T. 2013. Self-report of tobacco use status: Comparison of paper-based questionnaire, online questionnaire, and direct face-to-face interview—implications for meaningful use. *Population Health Management*, 17(3):186–189.

St Pierre, E. A. 2012. Another postmodern report on knowledge: positivism and its others. *International Journal of Leadership in Education*, 15(4):483–503.

Strauss, D.F.M. 2003. The Achilles' heels of positivism. *Koers: Bulletin for Christian Scholarship*, 68(2&3):255–278.

Swider, B.W., Barrick, M.R. & Harris, T.B. 2016. Initial impressions: What they are, what they are not, and how they influence structured interview outcomes. *Journal of Applied Psychology*, 101(5):625–638.

Sykes, L.M., Gani, F. & Dullabh, H. D. 2016. Principles of research study design: Understanding the options, indications and limitations. *SADJ* 71(7):319–323.

Tarin, E. 2017. Qualitative research and clinical methods. *Annals of King Edward Medical University*, 23(1).

Thales UK Ltd. 2013. Good Cyber is Good Business: The competitive advantage of cyber security. <http://news.bis.gov.uk/Press-Releases/Support-for-small-businesses-to-tackle-record-levels-of-cyber-attacks-68b5a.aspx>. Date of access: 09 June 2017.

- Thinyane, H., Sieborger, I. & Reynell, E. 2015. The potential of mobile phones for increasing public participation in local government in South Africa. *The Journal for Transdisciplinary Research in Southern Africa*, 10(3):241–259.
- Thompson, N., McGill, T. J. & Wang, X. 2017. Security begins at home: Determinants of home computer and mobile device security behaviour. *Computers and Security*, 70 :376 - 391.
- Tubaro, P. & Casilli, A., A. 2010. 'An Ethnographic Seduction': How Qualitative Research and Agent-based Models can benefit each other. *Bulletin de Methodologie Sociologique*, 105:59–74.
- Twinomurizi, H., Schofield, A., Hagen, L., Ditsoane-Molefe, S. & Tshidzumba, N.A. 2017. Towards a shared worldview on e-skills: a discourse between government, industry and academia on the ICT skills paradox. *South African Computer Journal*, 29(3):215–237.
- Twum-Darko, M. 2014. Factors influencing readiness for transformational e-government: a perspective of local government in South Africa. *Journal of Public Administration*, 49(2):513–523.
- Ukidve, A. & Tadvalkar, M. 2016. Analysis of management of information security and related enterprise risk in view of ISO/IEC 27001:2013. *Journal of Emerging Trends in Economics and Management Sciences*, 7(6):389–391.
- Unathi, M., von Solms, R. & Gerber, M. 2017. A Scenario-Based Information Technology Risk-Assessment for the Municipalities. *Journal of Public Administration*, 52(2):438–453.
- Uprichard, E. 2013. Sampling: bridging probability and non-probability designs. *International Journal of Social Research Methodology*, (16):1–11.
- van Rensburg, S.J. & Prinsloo, J. 2015. The criminogenic significance of social engineering and the need for information security. *Acta Criminologica: Southern African Journal of Criminology*, 45:89–106.

- van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J. & Kusev, P. 2017. Risk perceptions of cyber-security and precautionary behaviour. *Science Direct: Computers in Human Behaviour*, 34:707–716.
- van Solms, S. 2015. Ensuring safe networks through virtualisation: information security. *CSIR Science Scope*, 8:44–45.
- van der Spuy, I., Busch, A. & Bidonde, J. 2016. Interviewers' experiences with two multiple mini-interview scoring methods used for admission to a Master of Physical Therapy programme. *Physiotherapy Canada*, 68(2):179–185.
- van Zyl, I. 2015. Disciplinary Kingdoms: Navigating the politics of research philosophy in the information systems. *Electronic Journal of Information Systems in Developing Countries*, 70(1):1–17.
- Veiga, A., Asthakova, L., V., Botha, A. & Herselman, M. 2020. Defining organisational information security culture – Perspectives from academia and industry. *Computers and Security*: 1 – 52.
- Visser, B. 2015. Cyber Security risks, just as relevant locally as internationally. *Money Marketing* (12) :26.
- Waggett, P. 2013. Computer Security: Biometric Measures. *American Society for Engineering Education*, 23(1):17.
- Walsh, R. & Koelsch, L.E. 2012. Building Across Fault Lines in Qualitative Research. *The Humanistic Psychologist*, 40(4):380–390.
- Wempen, F. 2014. Computing Fundamentals. 3rd ed. Wiley Publishers: UK.
- Whitman, M., E & Mattord, H., J. 2012. Principles of information security. 4h ed. Cengage Learning: USA.
- Wisdom, P.J., Cavaleri, M.A., Onwuegbuzie, A.J. & Green, C.A. 2012. Methodological reporting in qualitative, quantitative, and mixed methods health services research articles. *Health Research and Educational Trust*, 47(2):722–745.

- Wonglimpiyarat, J. 2014. Innovative policies to support technology and ICT development. *Science Direct: Government Information Quarterly*, 31:466–475.
- Yasin, A., Liu, L., Li, T., Wang, J. & Zowghi, D. 2018. Design and preliminary evaluation of a cyber-Security Requirements Education Game (SREG). *Science Direct, Information and Software Technology* 95 :179–200.
- Yoo, C. S. 2011. Cloud Computing: Architectural and Policy Implications. *Review of Industrial Organisation*, 38(4):405–421.
- Yoon, D. 2017. The information science policy for the public open data of the national research institute. *Cogent business and Management*, 4:1–14.
- Young, R. 2016. Cyber security today and beyond. *HR Future*:32–33.
- Zhong, C., Lin, T., Lui, P., Yen, J. & Chen, K. 2018. A cyber security data triage operation retrieval system. *Science Direct, Computers and Security* 76:12–31.

APPENDIX A: SURVEY QUESTIONNAIRE

This questionnaire is designed to collect information from Information and Communication Technology (ICT) officials in City of Johannesburg (CoJ) and forms part of a study entitled “***A Managerial Framework for a Secure Computerised Environment in a Metropolitan Municipality***” at North-West University, Potchefstroom Business School. Your assistance and participation in this survey would be greatly appreciated and is completely voluntary.

The information that will gathered here will enable the ICT family in CoJ to understand and obtain a view on where we are in relation to ICT Security within the different entities in CoJ. Any information you complete in this questionnaire is confidential and nothing that you say will be personally attributed to you in any reports that results from this survey.

The questionnaire will be used for this study and will not be used for any other purposes. The demographic questions to the participants will be used in the statistical analysis for Frequencies, Descriptions and Comparative Analysis.

The questionnaire takes +- 20 minutes to complete.

For further information or clarification on any of the questions in the survey questionnaire or the entire research please don't hesitate to contact me on: itumeleng.mofikoe@gmail.com

My research supervisors can be contacted on the below email addresses:

1. Charles.VanDerVyver@nwu.ac.za
2. Christoff.Botha@nwu.ac.za

Section 1: Personal Background

Age:		Ethnicity:	
Highest Qualification:		Job Title:	
Years' Experience:		Gender:	Male
			Female

Section 2: Personal Awareness of Computer Related Issues

Please indicate your agreement with regard to the statements below by marking the appropriate number where the numbers indicate:

1 = Strongly Disagree, 2 = Disagree, 3 = Undecided, 4 = Agree, 5 = Strongly Agree

		Strongly Disagree	Disagree	Undecided	Agree	Strongly Agree
1.	I often use the internet to download music or programs	1	2	3	4	5
2.	I regularly check for viruses when I download a file or open an email attachment	1	2	3	4	5
3.	My firm uses programs to keep me from looking at Websites that are inappropriate for work	1	2	3	4	5
4.	There is nothing wrong with downloading music for free without permission	1	2	3	4	5
5.	There is nothing wrong with downloading videos for free without permission	1	2	3	4	5

6.	There is nothing wrong with downloading programs for free without permission	1	2	3	4	5
7.	When I have an important document for work, I save the file in more than one location (memory stick/CD/hard drive)	1	2	3	4	5
8.	I have reported to someone in authority when I was harassed or sent inappropriate material while online	1	2	3	4	5
9.	I often use instant message programs when I'm at work	1	2	3	4	5
10.	I often use chat rooms for work purposes	1	2	3	4	5
11.	I regularly buy items online	1	2	3	4	5
12.	I know how to tell if a website is secure and safe to give information to	1	2	3	4	5
13.	I often check for patches or other downloads for my computer to make it safer from hackers	1	2	3	4	5
14.	I disconnect from the internet when I am not using it	1	2	3	4	5
15.	I have used (or have come in contact with) a firewall or filtering software	1	2	3	4	5
16.	I use the same password for everything that needs a password	1	2	3	4	5
17.	I have used the internet to make fun of other people (or say bad things about them) because I knew no one would know it was me who did it	1	2	3	4	5

18.	When the allotted trial time has passed on software, I have downloaded (or borrowed) a 'crack' for it so I could continue using it for free	1	2	3	4	5
19.	I am concerned about someone stealing information about myself when I am online	1	2	3	4	5
20.	You can't get in trouble for changing someone's website because it's not real.	1	2	3	4	5

Section 3: Security Audit questionnaire

Please indicate your agreement with regard to the statements below by marking the appropriate number where the numbers indicate:

1 = Strongly Disagree, 2 = Disagree, 3 = Undecided, 4 = Agree, 5 = Strongly Agree

		Strongly Disagree	Disagree	Undecided	Agree	Strongly Agree
21.	The firm has cyber security policies based on industry standards.	1	2	3	4	5
22.	The firm has cyber security procedures based on industry standards.	1	2	3	4	5
23.	The firm protect sensitive information received from third-parties, with whom data is shared (I.e. Encryptions, SSL/TLS connections).	1	2	3	4	5
24.	Devices that store or process a third-party firm's sensitive information protected from the internet by a firewall.	1	2	3	4	5
25.	The firm has a designated Cyber-Security personnel	1	2	3	4	5

26.	Education and awareness programs on cyber-security are regularly performed in our firm	1	2	3	4	5
27.	External auditors performs cyber security audits in our firm	1	2	3	4	5
28.	Cyber security audits are performed at least once a year	1	2	3	4	5
29.	Systems are accessed with a unique user name and complex password	1	2	3	4	5
30.	Devices that store or process sensitive information have vulnerability scanning performed once a month	1	2	3	4	5
31.	Vulnerabilities are remediated in a risk based priority (highest priority vulnerabilities are fixed first)	1	2	3	4	5
32.	Devices that store or process sensitive information have patches updated within industry best practices (i.e.48 Hours) medium/ low risk Patches to be deployed in =<30 days?	1	2	3	4	5
33.	Devices that store sensitive information are encrypted	1	2	3	4	5
34.	Mobile devices (e.g. smart phones, tablets) that store sensitive information have a remote wipe functionality	1	2	3	4	5
35.	Mobile devices (e.g., smart phones, and tablets) that store sensitive information are accessed with a unique user name and complex password	1	2	3	4	5
36.	The firm has a Computer Incident Response Team (CIRT) to respond to cyber-attacks	1	2	3	4	5

37.	The firm has a formal process to respond to cyber-attacks					
38.	The firm requires a 2-factor authentication for remote access (e.g. a token used in addition to a username and password for a VPN login)	1	2	3	4	5
39.	The firm performs industry standard monitoring on devices that store or process sensitive Information	1	2	3	4	5
40.	The firm controls web access based on the risk (e.g. reputation, content, and security) of the sites being visited (E.g. Web Proxy controls)	1	2	3	4	5
41.	The firm actively participate in cyber-Intel sharing forums (e.g.ISAC, Infraguard)?	1	2	3	4	5
42.	The firm regularly performs phishing e-mail testing on its employees	1	2	3	4	5

Do you have any concerns relating to ICT (Information and Communications Technology) Security within your organisation?

Section 4: Management Questions (to be completed by the ICT Management teams)

43. On a scale of 1–10 (1 = bad & 10=good), do you have business buy-in and support towards the overall ICT Strategy?

1	2	3	4	5	6	7	8	9	10
---	---	---	---	---	---	---	---	---	----

44. What is your ICT Security cost (%) per annum in relation to the overall organisation costs? Provide details where possible

45. On a scale of 1–10 (1 = bad & 10=good), would you say business is deriving benefits from the costs attributed to ICT Security (ROI)?

1	2	3	4	5	6	7	8	9	10
---	---	---	---	---	---	---	---	---	----

46. Please elaborate on your response to question 45

47. On a scale of 1–10 (1 = bad & 10=good), do you have enough capacity and skills within your ICT department to address issues relating to ICT Security?

1	2	3	4	5	6	7	8	9	10
---	---	---	---	---	---	---	---	---	----

48. What is your biggest challenge at the moment regarding the overall ICT security within your organisation?

49. Are there any ICT Security risks or findings that have been identified by the auditors (internal/external in your most recent audits)?

50. If yes to question no 49, what is the plan in resolving the risks/findings identified?

51. On a scale of 1–10 (1 = bad & 10=good), how secure is your overall ICT Security platform within the organisation?

1	2	3	4	5	6	7	8	9	10
---	---	---	---	---	---	---	---	---	----

Thank you for completing the Questionnaire.

APPENDIX B: RESEARCH ARTICLE

DEVELOPING A MANAGERIAL FRAMEWORK FOR A SECURE COMPUTERISED ENVIRONMENT IN A MUNICIPALITY

Itumeleng MOFIKOE. North-West University, Business School, Potchefstroom Campus.
Potchefstroom, South Africa. itumeleng.mofikoe@gmail.com

Charles VAN DER VYVER. North-West University, School of Computer Science and
Information Systems, Vaal Triangle Campus. Vanderbijlpark, South Africa.
Charles.vandervyver@nwu.ac.za

Christoff BOTHA. North-West University, Business School, Potchefstroom Campus.
Potchefstroom, South Africa. Christoff.botha@nwu.ac.za

ABSTRACT

The primary objective of the research was to develop a management framework for a secured computerised environment in a metropolitan municipality. The literature review looked at the different elements that make up a secured computer environment, the characteristics of each element and how it could contribute to a secure computerised environment. It also highlighted what the United States of America (USA) and Europe have done in their computer security space. The meaning of cyber security for developing countries (in Africa) who are having more of their citizens increasing their internet usage on the different technology platforms was described.

A quantitative approach for collecting the data was adopted and the statistical analysis was done with the assistance of the statistical experts of a university. The results of the research were used to assist in the development of a framework that will ensure a secure Information and Communication Technology (ICT) environment in a municipality. The research revealed that even though there may be concerns generally around the ICT environment at the City of Johannesburg (CoJ), there is overall buy-in and a return on the investments done by the entities in support of their ICT strategy. The one aspect that requires improvement would be the capacitation for CoJ with specialised skills with specific focus on ICT Security.

Keywords: Computerised environment, Cyber security, Information security, Municipality, Managerial framework

1. Introduction

To increase the trustworthiness of the computing environments, a dependable approach to system development must be followed, which ensures that all the aspects of how that system can securely function are addressed.

Computing platforms are becoming more challenging each day and as a result, aspects of security requires improved defensive solutions. The situation leads to reasoning that structural engineers would never accept, such as claiming that obviously weak systems are ‘strong’ simply because we are ignorant as to which specific elements will fail (Kocher, 2016: 22).

Despite the progress (redesign and strengthening security programs) made in the security of traditional distributed systems, the securing of the computing systems poses new challenges due to the dynamic nature of such systems, e.g. topology not fixed, wireless network and the computation is context-aware. Security requirements are highly dependent on dynamically changing contexts such as user activity, location, nearby people and available resources (Siewe, 2016:121).

2. Problem Statement

With the advent of technology and more businesses investing in ICT to enable their business, secure computing environment requires specific focus and attention. Globalisation, the speed with which we do business and the mobility which the different technology platforms provide means that an municipality’s competitive edge and survival can be determined by the type of technology it has in place to conduct its business.

Thales UK Ltd (2013:2) in their study in the United Kingdom discovered that more companies are expected to come into contact with the threat of losing their confidential information through cybercrime. The number of breached companies in 2013 amounted to 93% of large companies with 87% of the small growing businesses having been victimised by cybercrime. These attacks normally result in major revenue losses and in some cases the total collapse of the business operations.

An independent study on Cybercrime by the computer security company McAfee in 2014 estimates that cybercrime costs South Africa around R5.8 billion per annum, which equates to 0.14% of the country’s Gross Domestic Product (GDP). Cybercrime is not only limited to large organisations and business institutions, but also extends to individual users of the Internet. A 2013 report by Symantec estimates that over 1 million South African citizens fall victim to cybercrime each year, making the Republic 3rd on the list of countries hardest hit by cybercrime (Mcdonald, 2015:47).

The US Government spends upwards of \$81 billion annually for their IT systems, components, software and related services, and it is highly reliant on IT to perform its many functions and responsibilities. This technological necessity is due to their recognition of a multitude of direct and indirect security threats against the government’s IT systems (Morrison, 2013:750).

According to Sorrentino et al., (2017:707), the digital agenda (especially e-Government policies) is one of the 7 pillars of the Europe 2020 Strategy which was launched by the European Commission in 2010 to set the goals and timeframes for the economic growth of the European

Union (EU). The Digital Agenda pushes EU member-states to fully embrace ICT's, not only Internet, but digital television and mobile telephony.

The challenge stems from the fact that technology has become part of our daily lives, and the majority of customers are becoming sophisticated from their improving interactions with technology in their everyday lives. With the gap in the digital divide closing, more people in societies are engaged on smartphones, tablets and online presence

The situation and conditions described above led to the formulation of the following research question, on which the research reported in this article pivoted: How could a managerial framework be produced that would provide a secure computerised environment in a metropolitan municipality?

3. Literature Review

Effective information security management cannot be realised without considering the roles of users and organisational attacks that originate from insiders. There are many users within the municipality that have legitimate capability to access one or many systems through authenticated processes. An insider may not necessarily be required to spend as much effort and time in accessing the targeted information in comparison to external attackers.

Attackers are developing sophisticated ways and means of avoiding detection based on the vulnerabilities in software and weak configuration of technical security countermeasures. Examples of security countermeasures include Network Intrusion Detection Systems (NIDS) which is capable of performing fine-grained network data and protocol-level analysis to identify anomalous and malicious traffic; and anti-virus tools that scan incoming software and attempt to match code signatures to a list of known malicious code bases (Burnap et al., 2018:400).

Ragaad (2010:5) emphasises that Information Security is now better understood by organisations because most of them have experienced in one way or the other, some harm produced by malware, intruders, or even their own employees. There's no single organisation that has not seen or experienced some undesired events that affected its computing environment and its information systems.

Thompson *et al.* (2017:376) acknowledges that accessibility of the Internet has provided an immense social benefit by linking communities and dissolving geographic boundaries. Even though communities have been brought together by developments in technology, this free, borderless communication has opened up new avenues for crime and fraud which exposes millions of computer users to cybercriminals across the globe.

Data that is transmitted may contain highly sensitive user information and to foster the widespread use of pervasive computing systems, it is critical to ensure that data that is exchanged is securely stored in these systems. With the advances in technology, handheld devices are getting smarter by the day, store more user information and can calculate the user's location at any time and communicate with the rest of the world through the Internet (Siewe, 2016:121).

According to Yasin *et al.* (2018: 179), the most crucial prerequisite for successful system development is understanding the security requirements of an organisation. Many researchers have a burning desire of making security requirements activities more engaging, enjoyable, and

rewarding in order to improve security requirements training/awareness and therefore increase its impact on the organisation.

ICT has brought about revolutionary changes in the way people work, communicate, learn, spend time and interact. ICT has also profoundly transformed business and government practices. The impacts of the ICT revolution are now palpable in all countries and are projected to be economically and socially revolutionary in the coming years as technology penetrates and fosters fundamental change in all sectors and dimensions of life (Jorgenson & Vu, 2016:383).

The business of securing computers, networks and the companies that use them is alive and well. Opportunities exist for information security professionals in corporate environments, security product vendor environments, government, military, educational institutions and professional services firms.

The words ‘cybersecurity’ may bring to mind international terrorism, corporate privacy and national security issues on all three spheres of government, however cybersecurity spans much more.

4. Development and Application of a Framework

Local governments, in addition to being close to citizens and business, constitute for many of them the main (or even unique) representation of government. The relationship of citizens and local authorities tends to be one based on proximity as the interests at stake for both parties are clearly entwined concerning issues such as public services, urban development, school planning, environmental concerns and local politics. It is at this level of local government that the impact of ICT on the relationship between governments and citizens, can be at its most effective and efficient (Misuraca, 2007:94).

The temptation nowadays is to limit ICTs to the computer and exclude other technologies such as radio, television and print. These technologies are readily available in homes and offices and have proven to be effective and inexpensive ways of enabling high-quality information to reach remote clientele and overcome geographical and cultural hurdles (Aderinoye, 2008:607).

Based on the literature review and challenges that exists within the ICT department of Municipalities, the following enablers are key to the formulation of a managerial framework for a secure computerised environment:

- ICT departmental roles
- Types/levels of skills required
- Technology platforms and applications
- Governance
- ICT strategies

5. Data Collection and Analysis

The research on the described objectives will be based on the literature review and an empirical study. A quantitative research methodology will be used in the form of a questionnaire that will be administered to the employees of the municipality to gain insight and their perspective on how secure they believe their computerised environment is. The research population in this study comprises of male and female employees in the ICT Departments of the various entities within the CoJ metropolitan municipality.

The physical questionnaire were all printed out and handed over to the ICT management team in the different entities for distribution amongst their team members. Participation in the study was completely voluntary and anonymous. The questionnaires were returned over a period of 2-3 weeks and once completed was handed over to Statistics department at the research university for the capturing of data and analysis.

In total, 80 questionnaires were issued to the participants and 71 completed questionnaires were received, amounting to a response rate of 88,75%. The remaining 9 questionnaires were not received back from the expected participants.

6. Empirical Investigation

Researches throughout the world typically ask two fundamental types of questions: (i) what is going on? (ii) Why is it going on? To answer the first question (what is going on) the researcher needs to examine the various philosophies, the use of literature in research and in the design techniques, integration of theory in research, and developing the theoretical perspective of research. The second question is answered through the framing of research questions under the qualitative, quantitative and mixed methods approaches and then illustrates how the various research designs are able to answer the basic research questions (Gurtoo, 2011:683).

It is important to note that as the organisations begin to compete in the global space and mature in their IT infrastructure and reliance on IT, this is likely to increase their risk in information security breaches. Organisations need to ensure that they have both the required technical and human skills required to ensure the safety of their organisations' computer environment. The focus of research is generally words, texts and images as opposed to gathering of statistical data (numbers) and using language focused on variables, with the goal of generalizing and confirming research hypothesis. However, these differing emphases do not mean that qualitative researchers do not use numbers or that quantitative researchers do not use words (Heser-Biber, 2016:6).

A qualitative researcher guided by a research question acts as an instrument, since the line of questioning may change during data collection as new understanding is gained and/or the situation changes. The data from research is derived from observation, interviews or verbal interactions, focus group discussions, document reviews, life histories, etc. and the researcher asks why, how and under what circumstances things occur; and not just what, where and why (Ensanullah, 2017:5).

7. Research Findings

The responses from the participants have been analysed using Frequencies, Descriptives, Reliability (which includes the mean, standard deviation and Cronbach's alpha) and T-test.

7.1 Frequencies

The research data established that out of a total sample, 56% are males while the remaining 44% are females. It must be considered though that due to the sample size of our research population, these numbers can't be extrapolated as the overall numbers for the ICT space in the City of Johannesburg.

7.2 Descriptives

The Research looks at the different responses from our participants in relation to the different sections of our questionnaire.

- **Personal Awareness**

This part of our analysis looks at how aware the participants are in relation to the personal experience of a computerized environment.

These sets of questions look at individual behaviour at work relating to downloads, online chatting and updating/awareness of computer viruses. The average mean is 2.80 which indicates that even though people make use of a computer and the internet in their daily lives, they are not particularly aware of the risks associated with their personal use of computers.

- **Security Audit**

This part of our analysis focuses on the aspects that relates to the security of the information in the organization.

The analysis on table 4.2 focuses on the participants' views on matters which may result in audit findings from both internal and external auditors in the municipality. The questions focus primarily on issues that relates to cyber security, system access, encryption on devices and any authentication that is required to access company systems. The average mean is 3.4 which indicates that respondents are fairly undecided or unclear on the role they should be taking on in the ICT department to ensure successful audit outcomes.

- **Questions relating to management only**

This part of our analysis looks at providing further information relating to the view of management on the business buy-in in the ICT strategy as well as whether they feel that the organization is deriving benefits from such investments. With regard to the issue of the business buy-in and support towards the overall ICT strategy, the mean was the highest with 6.38 which shows that management are average in agreement that there's a certain level of buy-in and support from the business with regard to their overall ICT Strategy.

The question relating to the having the required levels of skills/capacity to address ICT security issues, the mean was the lowest with 4.83 which demonstrates the concern from management on the skills that are required or currently lacking in the entities to address issues relating to ICT Security.

7.3 Cronbach's alpha, Mean and Standard Deviation

Cronbach's basic equation for alpha:

$$\alpha = \frac{n}{n-1} \left(1 - \frac{\sum Vi}{V_{test}} \right)$$

- n = number of questions
- Vi = variance of scores on each question
- Vtest = total variance of overall scores (not %'s) on the entire test
-
- **Effect size** – the measure which helps to describe the practical significance of the difference between the means of the two groups. The guideline for the effect size is as follows:
 - 0.2 small – no practically significant difference
 - 0.5 medium – practically visible difference
 - 0.8 large – practically significant difference

The Cronbach alpha values for all the grouped questions on the questionnaire are between 0.633 and 0.89. The lowest Cronbach is 0.633 for the Information Protection section and the highest one is 0.89 for the Free Downloads section. These constructs are considered reliable as all of them are above the guideline value of at least 0.5.

7.4 T-test

For the further analyses, Ethnicity were grouped into Africans (87.6%) and the Others which were made up of Coloureds, White and Indians (12.4%). The Research established that there are no practically visible or practically significant differences between the means of the Africans and other group, the highest effect size being 0.32 This small differences in the responses indicates that the respondents shares the same view with regard to the questions asked within each grouping.

8. Discussion

The primary objective of the research was to develop a managerial framework for a secure computer environment in a metropolitan municipality.

The managerial framework was developed using the research questions and the responses from the questionnaire. This framework demonstrates how the different areas of the questionnaire were responded to and this forms the basis of the recommendations in ensuring that the objectives of the study have been met. The managerial framework is depicted in figure 1.

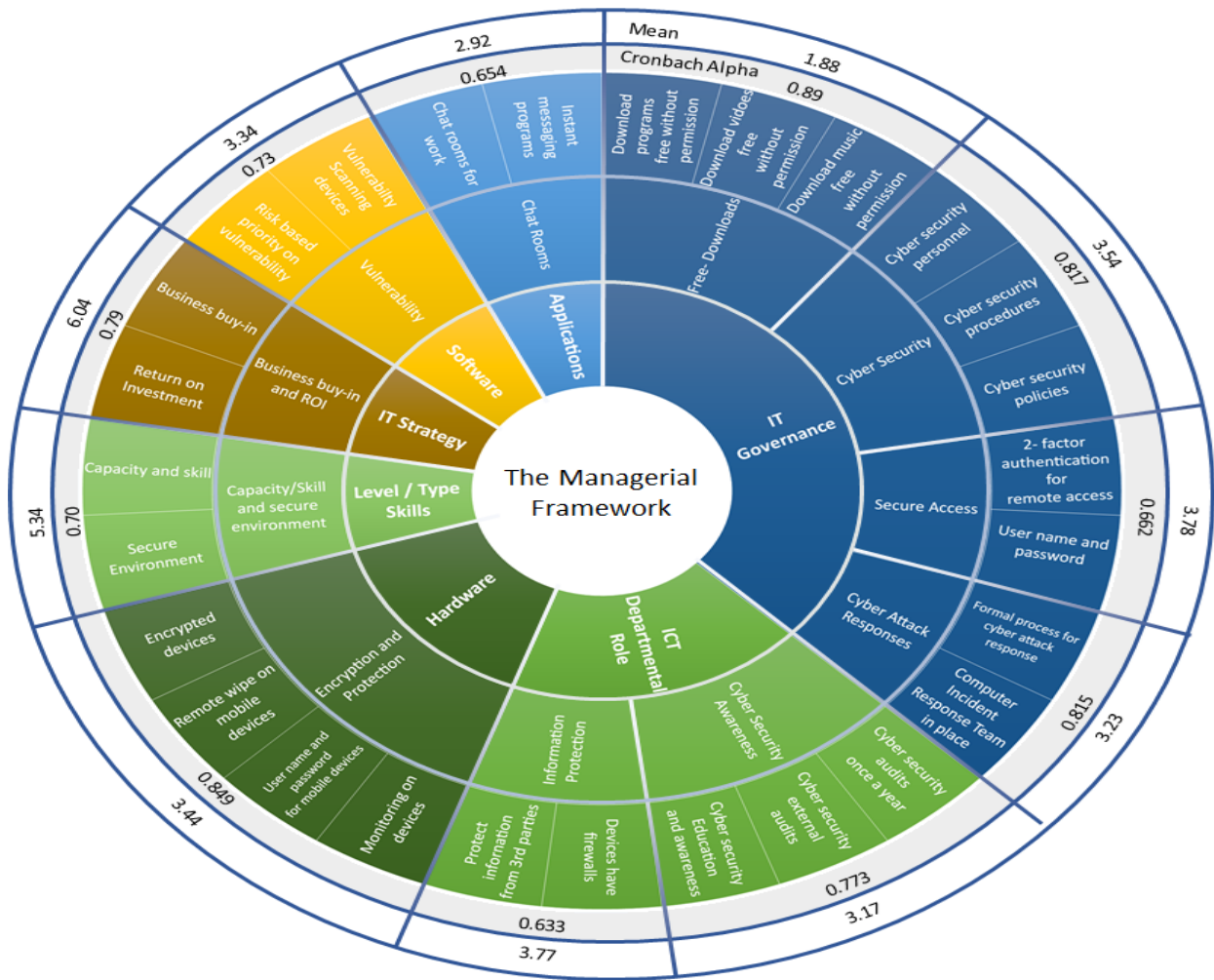


Figure 1: Managerial framework for a secure computerised environment in a municipality

The research aimed at also determining the role that an ICT department should take in the business and the required type and level of skill that will enable such a secure ICT environment.

The research looked at the personal awareness of each user and their experiences with regard to the usage of a computer and the internet at large. The research study then delved deeper into the area of audit which is critical for all municipalities as the Auditor-General conducts audits in municipalities looking at people, processes and technologies that are in place. The general responses indicate that even though the participants are aware of both internal and external audits conducted in their workplace – there's not enough awareness in terms of how they could each contribute towards clean audits in their ICT department.

Management must ensure that their ICT strategies are approved and implemented in their municipality. The implementation of such strategies requires investments in both financial systems and human capital to enable a secure computerized environment. Business no longer needs to look at ICT departments as just another support function, but rather a strategic partner which enables the business to leverage on the best available technologies in order to attain a competitive edge and as a result increase profits and/or quality of the service offerings that it provides.

9. Recommendations

The recommendations of the research emanate from the answers in response to our grouped questions from our questionnaire and the research objectives identified. The combination of the grouped questions and the research objectives were used in the development of the managerial framework. The recommendations listed below are based on the managerial framework developed which gets into the analysis of the questionnaire and the critical elements that need to be addressed in order to ensure a secure computerised environment.

The following list of recommendations should be implemented by all the ICT departments of the CoJ metropolitan municipality to ensure a secure computerised environment in the workplace:

- There should be a formal process in place to respond to any Cyber Attack threats
- A resourced and skilled computer response incident team should be a part of the ICT department
- Internal and External audits must be performed in the ICT environment at least once a year
- Cyber security education and awareness should consistently take place in the entire municipality
- All the ICT departments within the CoJ municipality should ensure that there are skilled security specialist within their teams
- All cyber security processes that are implemented should be compliant to all applicable laws, policies and standards
- All ICT policies within the municipality must be documented and approved through the applicable process of the municipality with their review periods/updates also indicated
- All company devices should be encrypted
- Mobile devices should have functionality that enables remote abilities
- ICT devices should all be accessed by independent usernames and passwords for all users of the systems
- Monitoring tools should be implemented on all the devices within the ICT infrastructure
- ICT infrastructure should be enabled with firewalls for all the devices within the environment
- All CoJ employees should not be allowed/permitted to download any programs, videos and music without permission
- Any remote access in the environment should be done using a 2-factor authentication
- All systems, platforms, databases and applications within the workplace, should be accessed with a username and password
- The ICT department must have staff for their environment with the required levels of skills and expertise for roles that are to be performed in the workplace
- There should be enough staff compliment in the ICT department to ensure that the environment is secured
- The ICT department should not be viewed as a support department but rather a strategic partner within the operations of the entire municipality
- The CoJ municipality should derive added business value and positive returns in the ICT investments that it has made to all the entities' ICT departments
- The returns and any added business value should provide the municipality with a competitive edge in its provision of services.
- Vulnerability scanning software should be in place in the environment and associated remedial actions , such as ensuring that scans are scheduled and performed and that any recommendations from the scans are followed and implemented

- A risk register for the ICT department should be maintained and updated at all times to ensure that sound controls are in place within the environment
- All CoJ employees should be encouraged to make use of secured instant message programs and chat rooms only for work related purposes and such restrictions should be communicated and enforced.

10. Indications for future research and conclusion

It is recommended that future research be expanded to the other metropolitan municipalities in Gauteng (City of Tshwane and Ekurhuleni). The expanded study will provide guidance on how other municipalities in the other provinces within the country have structured their computerised environments in order to meet their service delivery offerings to their citizens.

Further research can be done on the other developing (Brazil & China) and developed countries (USA and Germany) on how they offer services to their citizens making use of the technology environment that is available to them.

This research study has constructed a list of ICT guidelines that have been confirmed as being the most important to the development of a managerial framework in a computerised environment of a metropolitan municipality. This guideline was supported through the questions from our questionnaire that were grouped together in order to respond to the research questions of our study.

The study also seeks to contribute to the body of knowledge on ITC for a secure computerised environment in a metropolitan municipality in the following 4 ways:

1. By providing empirical evidence on the current state of a computerised environment in CoJ obtained from the perspective of the participants in the study
2. By making use of literature review to provide an understanding of the major concepts in ICT security
3. By developing a managerial framework that enables a secured computerised environment in the metropolitan municipality
4. By providing the entities Chief Information Officers with a series of recommendations that are associated with the managerial framework that have been proposed in the research study.

11. References

- Aderinoye, R. 2008. Literacy and Communication technologies: distance education strategies for literacy delivery. *International Review of Education*, 54: 605 – 626.
- Burnap, P., French, R., Turner, F. & Jones, K. 2018. Malware classification using self-organising feature maps and machine activity data. *Science Direct, Computers and Security*, 73: 399 – 410.
- Ehsanullah, T. 2017. Qualitative Research and Clinical Methods. *Annals of King Edward Medical University*, 23(1): 5 – 6.
- Flick, U. 2011. *Introducing Research Methodology: A Beginner's guide to Doing a Research Project*. SAGE Publishers, UK.

- Gurtoo, A. 2011. Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. *Current Science*: 101 (5): 683 – 684.
- Hesse-Biber, S. 2016. Qualitative or Mixed Methods, Research Inquiry Approaches: Some Loose guidelines for Publishing in Sex Roles. *Springer Science*, 74 (1) 6-9.
- Jorgenson, D., W. & Vu, K., M. 2016. The ICT revolution, world economic growth, and policy issues. *Science Direct, Telecommunications policy*, 40: 383 – 397.
- Ketefian, S. 2015. Ethical considerations in research. Focus on vulnerable groups. *Invest Educ Enferm*, 33(1): 165 – 172.
- Kocher, P. 2016. Privacy and Security. Computer Security is broken: Can better hardware help fix it? *Communications of the ACM*, 59(8): 22 – 26.
- McDonald, A. 2015. Accurate detection of intrusion in information networks: information security. *CSIR Science Scope*, 8: 46 – 47.
- Misuraca, G.C. 2007. ICTs for local government. 93 – 104.
- Punch, K. F. 2014. Introduction to Social Research Quantitative & Qualitative Approaches, 3rd edition. SAGE Publications, UK.
- Ragaad, B., G. 2010. Information Security Management, Concepts and Practice. New York: CRC Press.
- Raina, K. S. 2014. Self-weighting & non-probability samples. *Indian Journal of Medical Research*, 140: 149 – 150.
- Siewe, F. 2016. Towards the modelling of secure pervasive computing systems: A paradigm of context-aware secure action system. *J. Parallel Distribut. Comput* 87: 121 – 144.
- Sorrentino, M., De Marco, M. & Depaoli, P. 2017. ICT policies, the Mediterranean tradition and the Italian diet of discontinuity. *Science Direct: Telematics and Informatics*, 34: 707 – 716.
- Thales UK Ltd. 2013. Good Cyber is Good Business: The competitive advantage of cyber security. <http://news.bis.gov.uk/Press-Releases/Support-for-small-businesses-to-tackle-record-levels-of-cyber-attacks-68b5a.aspx>. Date of access: 09 June 2017.
- Uprichard, E. 2013. Sampling: bridging probability and non-probability designs. *International journal of social research methodology*, (16):1 -11.
- Yasin, A., Liu, L., Li, T., Wang, J. & Zowghi, D. 2018. Design and preliminary evaluation of a cyber-Security Requirements Education Game (SREG). *Science Direct, Information and Software Technology* 95: 179 – 200.