UNIVERSITY OF
KWAZULU-NATAL
INYUVESI
YAKWAZULU-NATALI

Assessing the Cyber-Security Status of the Metropolitan Municipalities in South Africa

by

Jerome Mabaso
941486884

**A dissertation submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy in
Information Systems & Technology**

College of Law & Management Studies
School of Management, IT & Governance

Supervisor: Professor Manoj Maharaj

2018

Declaration

I, Nkosiyephana Jerome Mabaso, hereby declare that:

(i) The research reported in this thesis, except where otherwise indicated, is my original work.

(ii) This thesis has not been submitted for any degree or examination at any other university.

(iii) This thesis does not contain other persons' data, pictures, graphs or other information, unless specifically acknowledged as being sourced from other persons.

(iv) This thesis does not contain other persons' writing, unless specifically acknowledged as being sourced from other researchers. Where other written sources have been quoted, then:

a) their words have been re-written but the general information attributed to them has been referenced;

b) where their exact words have been used, their writing has been placed inside quotation marks, and referenced.

(v) Where I have reproduced a publication of which I am an author, co-author or editor, I have indicated in detail which part of the publication was actually written by myself alone and have fully referenced such publications.

(vi) This thesis does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the source being detailed in the thesis and in the References sections.

Signed: …………………………………… 13 April 2018

N. J. Mabaso Date

Abstract

The intention of this enquiry was to assess the status of cyber-security in the metropolitan municipalities in South Africa. The focus on this level of local government was driven by the fact that metropolitan municipalities are the economic hubs with a variety of industrial facilities and are the places with high population densities. The metropolitan municipalities have adopted information infrastructures to support the daily administrative processes and, equally important, to support the delivery of essential services such as the distribution of electricity and clean water to the local citizens and communities. Entrenched in the adoption of information infrastructures are the cyber ills which if left unattended could have devastating consequences on people and industrial facilities. Failures or interruptions to information infrastructures have cascading effects due to interconnectedness of these infrastructures.

The study used the Constructivist Grounded Theory Methodology to explore the activities that are performed by the metropolitan municipalities with the intention to determine what needs to be in place to safeguard their information infrastructures from cyber ills. Cyber-security is a serious concern in all types of businesses that are largely supported by information infrastructures in pursuit of the business objectives. Information infrastructures are susceptible to cyber-security threats, which if left unattended can shut the municipality operations down with disastrous consequences.

A substantive theory of integrated development cyber-security emerged from the Constructivist Grounded Theory Methodology processes of data collecting through comprehensive interviews, initial coding, focused coding, memoing, and theoretical coding. A municipal cyber-security conceptual framework was developed from the integrated development cyber-security theory constructs of integrated development cyber-security which are the core category, cyber-security governance category, cyber-security technical operations category, and human issues in cyber-security category. The conceptual framework was used to formulate the cyber-security status assessment survey questionnaire that was adopted as an instrument to assess the cyber-security status in the metropolitan municipalities.

The cyber-security status assessment instrument was deployed in metropolitan municipalities, wherein data was collected and statistically analysed to test and confirm its validity. The assessment results were analysed and showed the as is posture of cyber-security, the gaps in the current implemented cyber-security controls were identified together with the risks associated with those gaps, corrective actions to address the identified deficiencies were identified and recommended/communicated to the management of relevant municipalities.

Summary

Title: Assessing cyber-security status in the metropolitan municipalities in South Africa

Candidate: Nkosiyephana Jerome Mabaso

Supervisor: Prof. Manoj Maharaj

Department: Department of Information Systems and Technology, in the School of Management, Information Technology, and Governance

Degree: Doctor of Philosophy in Information Systems and Technology

Keywords: Cyber-security, information infrastructure, critical information infrastructure, grounded theory methodology, Constructivist Grounded Theory, process control system, industrial control systems, National Cyber-security Policy Framework

Acknowledgements

My accolade goes to my supervisor, Professor Manoj Maharaj, for his guidance and encouragement along the research journey. He supported me by spending his valuable time, many hours indeed, reading through my draft thesis and providing valued comments. My time as a PhD student has been a challenging but at the same time fulfilling experience in my academic lifetime.

To my research participants, I salute all of you individually for giving your valuable time to be interviewed. If it was not for confidentiality reasons, I would have mentioned all of you by your name to express my gratitude to you all individually.

Dedication

To my wife, Phumzile, I don't have words that can translate the extent of my appreciation for your support that made me to endure challenges that are inherent to this type of endeavour.

My immense appreciation goes to my family, particularly my parents, Philemon Mabaso and Ellen Mabaso for the much needed support that they have provided to me in so varied ways to make me who I am. Finally but definitely not least, to my children, and grandson, I want you all to know that you are the reason why I have achieved this accomplishment. For helping and sustaining me throughout this endeavour, praise and thanks be to God Almighty.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

AGSA	Auditor General of South Africa
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIIP	Critical Infrastructure Protection
CIIs	Critical Information Infrastructures
CIs	Critical Infrastructures
ConGTM	Constructivist Grounded Theory Methodology
ENISA	European Network of Information Security Agency
EXCO	Executive Committee
GT	Grounded Theory
GTM	Grounded Theory Methodology
IDP	Integrated Development Plan
ICS	Industrial Control System
ICT	Information and Communication Technology
IRMSA	Institute of Risk Management of South Africa
IS	Information Systems
IT	Information Technology
ITU	International Telecommunication Union
KZN	KwaZulu-Natal Province of South Africa
MCCF	Municipal Cyber-security Conceptual Framework
MCII	Municipal Critical Information Infrastructure
MCIIP	Municipal Critical Information Infrastructure Protection
MFMA	Municipal Finance Management Act
MSA	Municipal Systems Act
NCPF	National Cyber-security Policy Framework
OECD	Organisation for Economic Co-operation and Development
PCS	Process Control Systems
SAPS	South African Police Service
SCADA	Supervisory Control and Data Acquisition (system)
SDBIP	Service Delivery Budget Implementation Plan
SIS	Safety Instrumented System

CHAPTER 1
RESEARCH INTRODUCTION AND BACKGROUND

1.1. CHAPTER INTRODUCTION

Chapter 1 has eleven sections. The sections covered are outlined in Table 1.1.

Table 1.1: Structure of Chapter 1

	Topic	**Overview**
1.1	Chapter introduction	Provides outline of the chapter.
1.2	Research background	Provides research context.
1.3	Research problem	What are issues that warrant this inquiry?
1.4	Research question	Precisely what the inquiry is about.
1.5	Research objectives	What are the intentions of this investigation?
1.6	Research rationale	Provides justification to execute this inquiry.
1.7	Theoretical framework	Synopsis of how this enquiry was conducted.
1.8	Research scope	Presents boundaries of this research.
1.9	Terminology used	Explanations of important concepts used.
1.10	Thesis outline	Provides road map of the thesis.
1.11	Chapter summary	Presents highlights of the areas discussed.

1.2. RESEARCH BACKGROUND

The South African Government published the National Cyber-Security Policy Framework (NCPF) in September 2015. The NCPF highlights the foremost considerations in protecting national cyberspace; on the other hand, it highlights the fact that there is no cyber-security implementation plan for the country. The study sought to make advances towards cyber-security implementation in the local sphere of government, specifically metropolitan municipalities. The NCPF includes statistics that list South Africa amongst the top three countries in the world that are targeted for phishing purposes (Mahlobo, 2015). The NCPF outlines broad policy guidelines on cyber-security in the country and it requires government to develop detailed cyber-security policies and strategies. In his speech for the Departmental Budget Vote 2016/17, South African State Security Agency Minister, David Mahlobo, highlighted the fact that the most cyber-attacks are now perpetrated by automated programmes which can run constantly with the intention of exploiting opportunities in various levels of government (Mahlobo, 2016). The Minister also stressed the fact that various structures that deal with cyber-security issues in the country have been established; however, these structures are inadequate in addressing cyber-security matters holistically (Mahlobo, 2015).

The country's current version of the National Development Plan (NDP) envisages that the ecosystem of services, applications, digital networks and devices will be integrated firmly into the social and economic fabric of the country (NPC, 2012). Amongst the major role players in the economy of the country, are the metropolitan municipalities. The risk that is associated with the implementation of digital and information and communication technology (ICT) is colossal and may impede or derail the attainment of the country's vision as per the NDP. Technological risks are becoming a serious problem for South Africa, particularly the escalation in large scale cyber-attacks together with an interruption of Critical Information Infrastructures (CIIs) (IRMSA, 2015). Critical cyber infrastructure interruptions to their intended functions can swiftly lead to disturbance in the real world such as water supply disruption, travel delays, electricity power supplies, financial difficulties, or even loss of human life. CII protection (CIIP) is an essential component of cyber-security because it is written or mentioned in relation to cyber-security in most National Cyber-security Strategies (GFCE, 2016).

The Internet Security Threat Report (Symantec, 2016a) highlights that vulnerabilities in industrial control systems (ICS) are likely to increase since these are connected to the Internet for remote control and monitoring (Symantec, 2016a). An example of an ICS is a supervisory control and data acquisition (SCADA) system. The reliance on CII has increasingly exposed the various government levels to threats that are inherent in the cyberspace. The local government sphere is the service delivery machine for the national government. The sophistication of threats to CIIs is real and emergent; hence criminal activity and service disruptions are becoming common (Hathaway, 2015). The real demonstration of the sophistication of threats in the cyberspace is the 2010 Stuxnet virus where CIIs such as ICS were attacked. South Africa urgently needs to act on the implementation of cyber-security strategies (Von Solms & Von Solms, 2015) as it cannot continue to drag its feet in protecting its cyberspace. Organisations' security and protection against cyber-ills remain major challenges (Dlamini & Modise, 2013).

1.3. RESEARCH PROBLEM

The increasing reliance of various levels of the South African government on CII has exposed government to considerable risk (Mohideen, 2016). Many cities around the world are aspiring to become smart cities, meaning that they want to enhance their usage of networked, digital technologies to address issues relating to improving service delivery and governance, creating more resilient critical infrastructure (CI), enhancing quality of life, growing the local economy, and more (Kitchin, 2016). The acceptable Smart City status is the one where a city uses digital technologies to enhance municipal performance and well-being, uses technology for reduction of costs, and to effectively and actively engage with its citizens (in.KNOW.vation, 2015). In South Africa, cyber-security research is critical because of the volatility and dynamic nature of the Internet (Grobler, Van Vuuren, & Leenen, 2012). Municipal CIIs are subject to a colossal variety of risks posed by cyberspace threats such as malware, intrusions of various kinds, distributed denial of service, hacking, viruses, spam, eavesdropping, and phishing.

Protecting CII is an area of concern worldwide since most countries use various critical systems which rely heavily on the Internet. Disruptions of the underlying information infrastructure, in turn, disrupt the proper functioning of these critical systems. The incidents in Estonia in 2007 that resulted in a series of distributed denial-of-service attacks were launched against several CIIs such that there were disruptions in government services and other critical systems, and disruptions in terms of access to financial institutions, brutally impacting on the nation's ability to function. In Georgia in 2008, there was also a cyber-attack on the CII which resulted in an inability of Georgian officials to connect with the outside world. These types of cyber-attacks present evidence on the inability of critical systems to function appropriately. Safeguarding CII is an issue of importance to every level of government. The increased complexity and connectivity of critical infrastructure systems are exploited by cyber-security threats, placing the government operations at risk (NIST, 2014). Local government have been left out in conversations on cybersecurity, and is abundantly apparent from the recent attacks by the SamSam ransomware attack that brought city services in Atlanta to a halt in March 2018 (Falco *et al.*, 2018)

Local governments are increasingly reliant on cyber-enabled technologies for various day-to-day municipal functions; underpinning these technologies should be resiliency, redundancy, and close scrutiny in order to circumvent harmful interferences to the service delivery mandate. The economic, security, health, safety, citizens' well-being, and effective functioning of all spheres of government, and, to some extent, even the survival of the industrialised private sector, rely heavily upon interconnected critical systems that are owned or operated by metropolitan municipalities. Due to the essential role to the country's security and economic operations, amongst others, the protection, stability, and reliability of interconnecting information infrastructures are no longer an option, but mandatory for various spheres of government. Local government's CII includes information infrastructures that support essential components that are vital to a national economy. CIIs mostly perform their functions through the support of ICT and ICS connectivity; and there is increased potential of cyber-vulnerabilities and risk exposures. Failure of these interconnected systems and assets could result in economic and social unrest (Dennis, Jones, Kildare, & Barclay, 2014).

Due to the lack of a framework to assist metropolitan municipalities to assess the municipal cyber-security status, the national remedial package and debate could be ineffective if it remains merely at the level of theoretical abstraction. There is a lack of cyber-security-related research in the country except the cyber-security awareness type of research (Grobler *et al.*, 2012). This situation could be exacerbated the by late promulgation in cyber-security policy in South Africa. Most efforts, as guided by the NCPF, are focused on promoting awareness which on its own is appropriate, however, obviously not sufficient. The research into this area is a timely necessity as cyber-threats are pandemic and no network interconnected system is automatically immune from them.

1.4. RESEARCH QUESTION

The NCPF focuses on national government, while other spheres of government are left out. Currently, there are no guidelines on sector-specific initiatives on how metropolitan municipalities should assess cyber-security status with the aim of cultivating the safeguarding of information infrastructures against cyber-security threats. The core research question that this study attempted to address is: What is the cyber-security status in South African metropolitan municipalities? The researcher mainly wanted to explore how metropolitan municipalities are protecting their municipal information infrastructures against cyber-security risks. The following sub-questions were formulated to provide solutions to the core question.

a. **How are metropolitan municipalities in South Africa protecting their information infrastructures against cyber-security threats?**

Metropolitan municipalities are at the local government level which is the sphere of government that is closer to people on the ground. Some of the day-to-day essential services such as water and electricity are delivered to the citizens. The day-to-day functional administration of these institutions are also supported by information infrastructures. In this enquiry the researcher wanted to determine the practices employed by these government institutions in safeguarding their information infrastructures against the risks posed by the cyber environment.

b. **What methodologies are currently available to assess the cyber-security status in the metropolitan municipalities in South Africa?**

Information infrastructures have been extensively utilised by metropolitan municipalities (at a local government level) to provide essential services to the citizens. To continuously provide these essential services, they (metropolitan municipalities) need to safeguard these information infrastructure assets against cyber-security threats. Once information infrastructure protection mechanisms have been implemented, then continuous assessment of their operational effectiveness becomes essential. Cyber-security assessment is conducted with the aim to cultivate cyber-security, and subsequently the protection of information infrastructure assets.

c. **How are metropolitan municipalities in South Africa inculcating the culture of cyber-security?**

Due to dependency of these government institutions on information infrastructures, it is expected that the protection of information infrastructure assets is at an acceptable level. To preserve the information infrastructure protection, these government institutions are executing pertinent processes to achieve the acceptable level of cyber-security. To maintain an acceptable level of cyber-security requires a culture that promotes the protection of information infrastructure assets. Cyber-security culture is one of the important components that provides and sustains an enabling environment for the protection of information infrastructure assets.

d. **What theoretical framework supports cyber-security implementation in the metropolitan municipalities in South Africa?**

The cyber-security phenomenon is fairly new compared to the related information security phenomenon. Due to the criticality of cyber-security, the researcher considered it imperative to seek explanations about cyber-security implementation in the metropolitan municipalities. The researcher wanted to determine what these government institutions do to implement cyber-security, and why they do what they do to safeguard the information infrastructures against cyber-risks.

e. **How can metropolitan municipalities in South Africa successfully assess their cyber-security status?**

An instrument or tool is required to conduct an assessment of cyber-security status. The assessment tool must produce assessment results that guide management in the decision-making process. Due to the sensitive nature of cyber-security, successful assessment of its status within these government institutions is believed would cultivate information infrastructure protection against cyber-threats.

Cyberspace ills have the potential to shut down the operations of the metropolitan municipalities in the country, and, therefore, a risk management approach towards protecting the cyberspace is considered as one of the tools for securing the interconnected CII upon which the local governments rely so heavily for their day-to-day business operations. The country's CII and networks are exposed to unprecedented cyber-attack levels (IRMSA, 2015).

1.5. RESEARCH OBJECTIVES

The digitisation of government operations and associated service delivery mechanisms offers many opportunities, but risks of disruption of essential processes for production, logistics and services also increase. Assessing the status of cyber-security in the metropolitan municipalities is envisaged to enhance cyber-threats awareness, cyber-related information and knowledge sharing, and joining forces to protect and improve responsiveness of information infrastructures. The study aimed to enhance the protection, resilience, and reliability of metropolitan municipalities' information infrastructure assets. The ever-increasing innovation in cyberspace necessitates better approaches and procedures to understand, monitor and safeguard information infrastructures against cyber-security threats.

The study's core objective was particularly in determining the cyber-security status in South African metropolitan municipalities. To achieve the research core objective, the following sub-objectives were identified.

a. **To explore the practices that metropolitan municipalities in South Africa have implemented to protect their information infrastructures against cyber-security threats**

   It is important to understand the posture of cyber-security before any enhancement mechanisms can be effected. The ConGTM study as presented in Chapter 4 was conducted to achieve this research objective.

b. **To explore the methodologies currently employed to assess the cyber-security status in the metropolitan municipalities in South Africa**

   The researcher aimed to explore the practices currently adopted with the intention of assessing the cyber-security status in metropolitan municipalities in the country. The intention to assess the status of cyber-security culture included:

   (i) understanding the "as is" situation in order to draft the road map of getting into the desired destination to successfully protect the information infrastructure assets;

   (ii) changing or enhancing the existing culture of cyber-security within the institution; and

   (iii) maintaining the current practices employed to protect information infrastructure against cyber-threats.

   This research objective was achieved through the use of the ConGTM processes as presented in Chapter 4. The practices are presented in the form of focused codes that are pertinent to addressing this research objective.

c. **To understand the processes that are employed to provide an enabling environment to develop, implement, and sustain cyber-security culture in metropolitan municipalities in South Africa**

Identifying the processes employed to make the environment conducive for the information infrastructure protection is important. A conducive environment is made possible amongst other domains by the appropriate culture. These processes are explained also in Chapter 4.

d. **To develop a theory that explains cyber-security implementation in the metropolitan municipalities in South Africa**

A substantive theory was developed to achieve this research objective and it is discussed in Chapter 5. The emerged substantive theory presents the rationale for cyber-security implementation in metropolitan municipalities in South Africa. This substantive theory integrated ideas and hypotheses that account for cyber-security implementation in the metropolitan municipalities in South Africa.

e. **To develop an instrument to successfully assess cyber-security status in metropolitan municipalities in South Africa**

The conceptual framework that was developed is presented in Chapter 6 forms the foundation in the development of a cyber-security assessment tool in metropolitan municipalities in South Africa. The conceptual framework was developed from the ConGTM processes discussed in Chapter 4 and Chapter 5. A cyber-security assessment instrument that was developed is presented in Chapter 6. Chapter 7 empirically applies the developed cyber-security assessment tool to assess the status of cyber-security in the metropolitan municipalities in South Africa.

1.6. RESEARCH RATIONALE

The government-integrated information infrastructures' evolution has created new, exploitable, cyber-security vulnerabilities and this necessitates a heightened sense of urgency for the safeguarding of information infrastructures against cyber-threats. Cyber-security controls such as ICT service continuity, security management and user access are the areas that need attention when it comes to the status of controls in South African municipalities (AGSA, 2014). The country has become dependent on the Internet to govern and conduct its day-to-day government business functions (Mahlobo, 2015). A national understanding at the level of municipalities is necessary for strengthening and advancing the NCPF objectives and this research will, hopefully, contribute towards such an objective. The study focused on empirical evidence to assess cyber-security capacity at metropolitan municipal level of local government in the country. The research has followed a call by the National Minister of State Security (through the NCPF) that there is no cyber-security implementation plan for the country, and, as such, it is the aim of this study to contribute towards a cyber-security implementation plan.

Municipalities are the level of government that have the most direct impact on the day-to-day lives of South African citizens through the provision of services such as refuse removal, electricity, water, and sanitation, amongst others. ICT is one of the enablers towards the implementation of NDP and supports government's efforts to uplift its citizens. This research is intended to support the government initiatives at metropolitan levels to implement and operationalise the NCPF. This study recognises the NCPF intentions; and at the heart of this research is the intention to advance the protection of the country's information infrastructures that are found in the sphere of local government, particularly in metropolitan municipalities. The NCPF outlines broad policy guidelines on cyber-security in the country and it requires government to develop detailed cyber-security policies and strategies and this research was envisaged to close this gap. A further aim of the study is to broaden and to strengthen the knowledge base in the cyber-security field. Cyber-attacks on information infrastructures can have devastating consequences for human lives and the environment. It is vital that efforts are continuously made to enhance the protection and resilience of such infrastructures.

The significance of the study is its central thrust on theory development to be applied to guide metropolitan municipalities in addressing the cyber-security challenges. The current NCPF addresses cyber-security at national government level only, leaving local government unattended and by extension vulnerable. This study was prompted by the realisation of the fact that there is no coordinated approach to dealing with cyber-security in South African local government environments. For this reason, it could be argued that this research comes at an opportune time, given the extent and likelihood of cyber-related risks on the provision of essential services that the metropolitan municipalities deliver to the citizens. Hopefully, the municipalities may use the cyber-security framework developed from this study, preferably on a continuous basis (preferably annually) to assess capacity and implement recommended measures to enhance information infrastructure cyber-security. The developed cyber-security framework can also be adapted to and used by other types of municipalities in the country.

1.7. THEORETICAL FRAMEWORK

The research process for this study comprised two phases, namely Phase I and Phase II. The study made use of mixed methods research which included the qualitative and the quantitative approaches, respectively. The two primary goals of the study were to develop the applicable theory and subsequently to formulate a conceptual framework that describes the phenomena, and secondly, to verify the conceptual framework that explains the phenomena. A mixed method research was adopted to achieve conclusive findings of the study. Firstly, through a qualitative approach, semi-structured interviews were used to collect data, and subsequently ConGTM of creating open codes, focused codes, and theoretical coding was employed to analyse the data. Secondly, quantitative data, using a structured survey questionnaire, was collected and analysed by means of statistical analysis. The adoption of the mixed method approach in this research improved the rigour and explanation of the research results, as both studies confirmed the same research finding, thereby bringing to the fore conclusive findings to the study outcome.

Phase I of the study was the qualitative study that employed the ConGTM. Due to the lack of existing theory regarding cyber-security capacity assessment at metropolitan municipalities, ConGTM was regarded as the best fit for this study. ConGTM offers a qualitative analysis to develop a new theory that is based on collected empirical data. The grounded theory defining characteristics include reliance on empirical data, conceptual abstraction, openness to emerging ideas, and critical analysis (Strauss & Corbin, 1998, p.7). The process of developing theory is the basic tenet of grounded theory. Avoidance of using pre-formulated hypotheses and preconceived theories are other characteristics of GTM. The application of GTM is evident in the work of Charmaz (2006), Allan (2007), Urquhart (2007), Urquhart, Lehmann, and Myers (2010), and Urquhart and Fernandez (2013).

In implementing the grounded theory, several approaches can be pursued including the following:

(a) Glaserian Grounded Theory was named after the one of the originators, Barney Glaser. This approach requires the postponement of the literature review process until completion of data analysis and theory generation (Glaser & Strauss, The discovery of grounded theory: Strategies for qualitative research, 1967). This was considered as not appropriate for this study since the University's research protocol requires a preliminary literature review before the research proposal can be approved. This approach also operates from the viewpoint that during the research process the researcher should keep a critical distance from the study in order not to introduce bias and preconceived ideas. This viewpoint was not in line with the researcher's philosophy of being the active participant in the research.

(b) Straussian Grounded Theory was named after Anselm Strauss, who worked with Corbin to argue that the GTM as a tool of research should evolve, and they recognised the bias that may creep in from preconceptions of the researcher (Strauss & Corbin, 1998). According to Strauss and Corbin (1998), when it comes to researcher objectivity, they take the middle ground. The researcher, according to them, cannot start an inquiry without pre-conceptions of some sort; they, however posited that the inquirer be as objective as possible during data collection. The view of this strand is that the researcher is not the active participant. The data collection and analysis processes follow a stringent set of steps which in a way limits researcher creativity as an active participant.

(c) Charmaz's Constructivist Grounded Theory was named after Kathy Charmaz (2006), according to whom, both Glaser and Strauss are positivists who treat the researcher as an observer who is distant when collecting data (Charmaz, 2006). During collection and analysis of data, the constructivist grounded theory approach subscribes to the belief that the interviewees and researcher jointly co-construct meaning and hence the researcher of this study opted to follow this perspective in executing this enquiry. The researcher's view was to take into consideration that metropolitan municipalities are social entities. Charmaz (2008) posited that "A social constructionist approach to grounded theory allows us to address *why* questions while preserving the complexity of social life. Grounded theory not only is a method for understanding research participants' social constructions but also is a method that researchers construct throughout inquiry" (Charmaz, 2008, p. 397).

The adoption of ConGTM in this investigation was based on the work of Lehmann (2010), who argued that grounded theory (GT) is an appropriate research method in information systems (IS) because the IS field interacts with people, technology, data, and procedures which are varied components. GT was the best fit because of the core to this investigation, which was to assess cyber-security capacity at metropolitan municipalities in South Africa. GT is an applicable research method for IS because of its systematic and rigorous approach to research (Allan, 2007).

The study did not make use of predefined theoretical frameworks as a starting point; instead, the study followed an inductive approach to explore this research area from a fresh perspective. The initial data for this study was collected through in-depth interviews conducted to examine activities that are performed by role players in cyber-security processes within the municipalities. Phase II was a quantitative study that employed a survey questionnaire with structured questions. In Phase I, the enquiry used semi-structured interviews to explore how individuals described the phenomenon, and used the findings from this phase to develop statements that were employed to formulate structured questions to collect data quantitatively. The objective of adopting this design was to generalise qualitative findings to a larger sample. The rationale for utilising this design included: instruments are not available to assess the status of cyber-security in metropolitan municipalities; the variables for the instrument are not known yet; and lack of theory or model to serve as a guide was a key consideration.

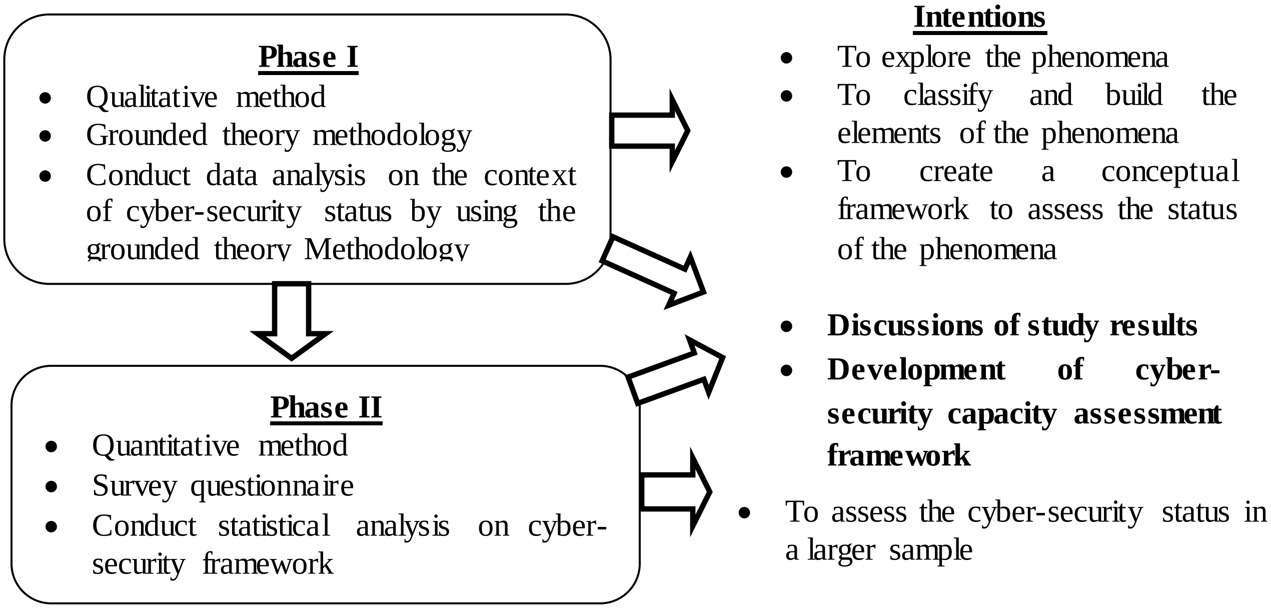

Phase I
Qualitative method
Grounded theory methodology
Conduct data analysis on the context of cyber-security status by using the grounded theory Methodology
Phase II
Quantitative method
Survey questionnaire
Conduct statistical analysis on cyber-security framework
Intentions
To explore the phenomena
To classify and build the elements of the phenomena
To create a conceptual framework to assess the status of the phenomena
Discussions of study results
Development of cyber-security capacity assessment framework
To assess the cyber-security status in a larger sample

Figure 1.1: Research methodology model

1.8. RESEARCH SCOPE

This research focused on information infrastructures that are owned by metropolitan municipalities in the country. Information infrastructure covers information and communication technology (ICT), and process control systems (PCS) and networks which form an important link in the chain of guaranteed supply of essential services to the citizens of the country. It is imperative that metropolitan municipalities are in control of the process automation environment particularly because PCS are largely dependent on ICT to function effectively. Figure 1.2 presents the scope of the inquiry.

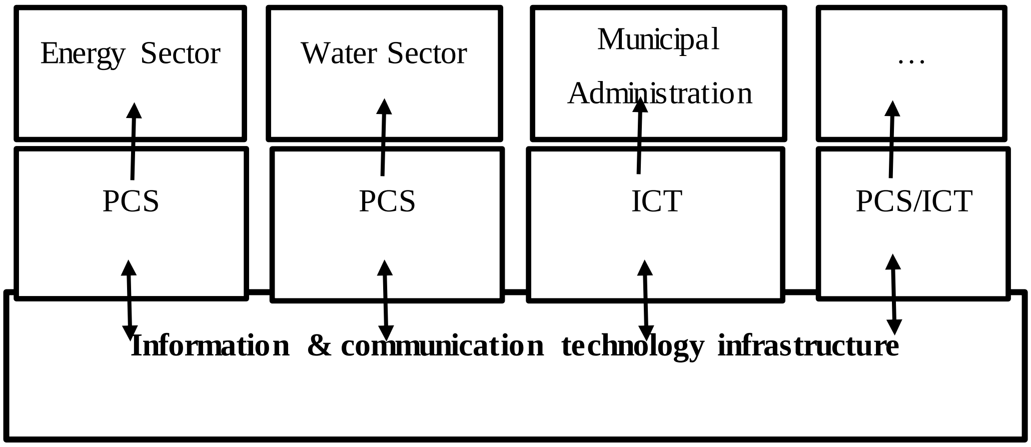


Figure 1.2: Research scope

1.9. TERMINOLOGY USED

This research adopted an understanding of various concepts as defined and discussed in the following sections.

1.9.1. Cyber-security

NCPF describes cyber-security as the practice of securing networks that constitute cyberspace against intrusions, to maintain information confidentiality, integrity, and availability; detecting intrusions, responding to and recovering from them. ITU (2008, p. 2) provides a broader definition as it explains cyber-security as a

> "*collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and*

> *technologies that can be used to protect the cyber environment and organization and user's assets"* (ITU, 2008).

In the context of this enquiry, cyber-security was viewed as defined above. Also, the NCPF has adopted the same definition from ITU.

1.9.2. Information infrastructure

According to the South African cybercrimes and cybersecurity bill published in the Government Gazette No. 40487 of 9 December 2016, information infrastructure means "any data, computer program, computer data storage medium, computer system or any part thereof or any building, structure, facility, system or equipment associated therewith or part or portion thereof or incidental thereto" (RSA, 2016, p. 41). This enquiry adopted this definition of information infrastructure. The focus of the study was on information infrastructure, that its operational functionality which is the responsibility of metropolitan municipalities in the country.

1.9.3. Critical information infrastructure

In this enquiry, infrastructures refer to man-made systems that operate interdependently to generate and dispense vital goods (such as water, energy, and data) and services (such as banking, transportation, and healthcare). NCPF views infrastructure as critical if its inability or damage has a major impact on government administration, health, safety and security, economic and social well-being of the citizens. NCPF acknowledges the need to safeguard CII in order to achieve the continued provision of essential services and support security, economic prosperity and social well-being. Technology and related information has become a central part of the CI. A number of the municipal essential services are gradually becoming dependent on IT.

1.9.4. Assessing cyber-security status

To assess means "to make a judgement about the nature or quality of something" (Oxford Dictionary, 2006). This enquiry sought to determine whether the level of cyber-security status in the municipalities is adequate to provide a quality (successful) safeguard to information infrastructures. Cyber-security status that is at an acceptable level is defined as one that delivers sufficient safeguard to an organisation's information infrastructure. It is essential that the cyber-security status assessment instrument is credible to yield results upon which management can base their decisions. The process of assessing cyber-security status in an organisation cultivates cyber-security and subsequently promotes information infrastructure protection.

1.10. THESIS OUTLINE

This research thesis consists of nine chapters. Chapter 2 presents background literature that the researcher reviewed for this enquiry. Chapter 3 discusses the research method that was followed in executing this study. Constructivist Grounded Theory Methodology was the chosen method to conduct this research. Chapter 4 presents the research study site and data analysis for the qualitative part of the enquiry. EThekwini Municipality was conveniently chosen as the study site. Chapter 5 discusses the emergent theory wherein theory variables are discussed. Chapter 6 presents the development of the municipal cyber-security framework. Chapter 7 discusses the development of and empirically tests the municipal cyber-security assessment tool. Chapter 8 deals with the process for assessing the cyber-security status. Lastly, Chapter 9 is the concluding chapter of the study which includes the contribution of the research, its limitations, and makes suggestions for future research.

1.11. CHAPTER SUMMARY

Chapter 1 mainly discussed the context of the inquiry. A high-level view of the position of the country on cyber-security was provided. Furthermore, the research problem of the study was contextualised; the need to safeguard the municipal information infrastructure was presented; and the research question was posed as follows: How can metropolitan municipalities in the country successfully assess cyber-security capacity? In addition, the research objectives were discussed; the rational to conduct this enquiry was provided; the methodology to execute the study was discussed, including as discussion of GTM and ConGTM which was chosen as the methodology to follow to conduct the research; and the scope of the enquiry was presented with the research focus and boundaries being discussed. Finally, the chapter provided definitions of key concepts that have been used in the research and lastly, the thesis outline was presented.

CHAPTER 2
LITERATURE REVIEW

2.1. CHAPTER INTRODUCTION

This chapter presents the extant literature in the area under study. In academic research, reviewing current literature seeks to highlight the conceptual background. In the final part of the research, the literature review guides the research findings and discussions. Charmaz (2006, p. 165) argued that the literature review helps in identifying gaps in current research works, and adds context to the study. The researcher approached the literature review with a critical mind. The literature review assisted the researcher to identify a gap in the area of interest which was then used to develop the research questions. The researcher did not have a preconceived theory in mind nor any pre-formulated judgement about the phenomenon being investigated before embarking on this enquiry.

There are 11 sections discussed in this chapter. Table 2.1 presents the chapter outline.

Table 2.1: Structure of Chapter 2

	Topic	**Overview**
2.1	Chapter introduction	Provides context to the chapter.
2.2	Various views on cyber-security	What is happening in the sphere of cyber-security?
2.3	International organisations on cyber-security	What are international views on cyber-security?
2.4	RSA NCPF	What is the position of the RSA on Cyber-security?
2.5	CII	Impact of cyber-security on CII.
2.6	Attack on critical infrastructure: Stuxnet Worm	Effect of cyber on PCS.
2.7	Differences between IT security and cyber-security	Cyber-security is beyond IT security.
2.8	Current cyber-security research perspectives	RSA cyber-security research perspectives.
2.9	Cyber-security statistics in South Africa	What has Africa been exposed to?
2.10	Local government legislative framework in South Africa	Why focus on metropolitan municipalities?
2.11	Chapter summary	Provides highlights dealt with in the chapter.

The prevailing South African NCPF highlights certain considerations in protecting national cyberspace. However, some of the critical information infrastructures are found within the jurisdiction of local governments in various municipalities. A national understanding at the level of municipalities is necessary for strengthening and advancing the NCPF objectives. This research recognises the aims of NCPF and the core intention of this study was to enhance protection of critical information infrastructure at a local government level. The local sphere of government is the service delivery machine for the national government. Due to the lack of a framework for assessing municipal cyber-security capacity, the national remedial package and debate could be ineffective, if it remains merely at the level of theoretical abstraction.

2.2. VARIOUS VIEWS ON CYBER-SECURITY

All levels of government exist mainly to safeguard property and the lives of the citizens, to facilitate commerce and to maintain social order. Cyber-security is a national security matter due to the illegal use of cyberspace that could result in devastating consequences for national security functions (Wamala, 2011). Some nations across the world have published their national cyber-security strategies and policy frameworks, amongst which are the United Kingdom (UK), Uganda (UGA), Spain (ESP), South Africa (ZAF), New Zealand (NZL), the Netherlands (NLD), Romania (ROU), Luxembourg (LUX), Lithuania (LTU), Japan (JPN), India (IND), Germany (DEU), France (FRA), Estonia (EST), Czech Republic (CZE), Canada (CAN), and Australia (AUS) (Luiijf, Besseling, & De Graaf, 2013). All these nations have defined cyber-security in different ways, thus there is no synchronised, common definition on cyber-security across the nations.

Table 2.2: Definitions of cyber-security by various nations

	Country	Definition
1	ZAF	[involves] the risk management approaches, assurance, policies, safeguards, best practices, training, tools, actions, and technologies used to secure the cyberspace, organisational assets and users
2	UGA	is the safeguarding of information systems and information from illegitimate access, disruption, use, modification, disclosure or destruction (references to information security)
3	ROU	is a set of measures to ascertain information authenticity, integrity, confidentiality, non-repudiation and availability, protecting the cyberspace, [and both] public and private resources

	Country	Definition
4	NZL	is the practice of protecting cyberspace and related components against attacks, maintaining information availability, confidentiality and integrity, detecting cyber-attacks that occur and recovering from such malicious incidents
5	NLD	is to protect ICT from the dangers of abuse, destruction or disruption
6	IND	is the safeguarding of information systems, networks and information with relevant technological measures against abuse, destruction or disruption
7	GBR	is the safeguarding of national interests in the utilisation of cyberspace, and the wider national security policy pursuit
8	FRA	is the protecting of cyberspace from events that may compromise information and systems integrity, confidentiality, availability and other related services that are offered by IT systems
9	DEU	is the achieving of a necessary situation in protecting IT in which cyberspace risks are reduced to the minimum acceptable [level]
10	CAN	is the mitigation of risks resulting from cyber-attacks, implementation of adequate response level from cyber-incidents, such as the illegitimate use, access, manipulation, disruption or destruction of electronic information and related infrastructure
11	AUS	are information-protecting mechanisms that preserve information integrity, confidentiality and availability that is stored, processed and transmitted by electronic or related means

Source: Luiijf, E., Besseling, K., & De Graaf, P. (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures*, vol. 9, numbers 1-2, p. 6.

What is common to most of these definitions is the issue of the threat posed by cyber-attacks on CIIs. CIIs are cyber-based systems that are critical for the daily functioning of the government at various levels and for the country's economy (Ralston, Graham, & Hieb, 2007). Cyber-security definitions vary and the term is used broadly (Craigen, Diakun-Thibault, & Purse, 2014).

2.3. INTERNATIONAL ORGANISATIONS ON CYBER-SECURITY

2.3.1. The International Organization for Standardization (ISO)

The International Organization for Standardization (ISO) is a non-profit organisation that develops and publishes standards of virtually every possible type, including cyber-security. ISO which was founded in 1946 is supported by 159 countries and is the leading issuing body for international standards (Disterer, 2013). The standards ISO 27000 to ISO 27002 were developed in cooperation with the International Electro-technical Commission (IEC), which is a leading global issuer of international standards in the electronics and electronic-related technologies sector

ISO 27032 (ISO/IEC, 2012) is the cyber-security standard that is recognised globally and was designed to address the lack of communication between cyberspace users and providers (Dennis *et al.*, 2014). According to the ISO/IEC 27032 (ISO/IEC, 2012), the standard was designed to address the reality that

> *Devices and connected networks that support cyberspace have multiple owners – each with their own business, operational and regulatory concerns. Not only do the different users and providers share little or no input, but each has a different focus when dealing with security. Such a fragmented state opens up vulnerabilities in cyberspace. ISO/IEC 27032 will provide an overarching, collaborative, multi-stakeholder solution to reduce these risks.*

This framework provides guidance on four domains, namely information security, internet security, network security and critical information infrastructure (ISO/IEC, 2012).

2.3.2. International Telecommunication Union (ITU)

The United Nations has a specialised agency responsible for ICT across member states called the International Telecommunication Union (ITU). ITU has recognised the criticality of cyber-security and the possible adverse consequences of any inefficiency. As a result, the Union constructed the *Global Cyber-Security Agenda (GCA) Strategy Guide* (ITU, 2015). The GCA is a framework prescribed for utilisation by all interested countries and is independent of international barriers. The guide aims to design, implement and provide strategies on cyber-security across different sectors. The GCA framework provides a holistic development, implementation and coordination of a vigorous global cyber-security culture (ITU, 2015). The Ends-Ways-Means strategy was used to address the issue of cyber-security (Dennis *et al.*, 2014). As the basis for cyber-security strategies, ITU recommends that countries apply national values, since countries have varied needs, capabilities and threats. The ITU (2015) recommendations are based on:

a. the perception that risks and their mitigations are influenced by national interest and culture; and

b. a country's relevant stakeholders on cyber-security, such as private and public sectors and the judiciary are likely to support the strategy since it is rooted in the national interests and values.

2.3.3. Organisation for Economic Co-operation and Development (OECD)

The Organisation for Economic Co-operation and Development (OECD) is an international forum where governments across the globe work together to attend to issues concerning economic, environmental, and social challenges globally. The OECD is a neutral setting where member states collaborate, seek to formulate solutions for common challenges, formulate best industry practice and function to coordinate international and domestic policies (OECD, 2015). ICT and the Internet are critical for social and economic development; hence they are part of critical infrastructure. On the other hand, cyber-security policy formulation is in its infancy (OECD, 2015). The organisation takes cognisance of the fact that governments are hugely dependent on digital infrastructure to execute fundamental service-delivery functions. Threats to cyberspace are surfacing rapidly and the cyber-attackers appear to be better organised as they conceal their tracks. The high extent of sophistication, such as that of Stuxnet, is clear confirmation that governments are faced with a daunting task of protecting critical information infrastructure. Governments need to adopt an integrated and comprehensive approach when addressing cyber-security policy issues, particularly taking into consideration the essential impact of the Internet and related technology on the modern economy (OECD, 2015). Facets of cyber-security need to be addressed holistically, covering government-wide applications and also encompassing the social, economic, legal, educational, technical, law-enforcement, diplomatic, intelligence and military-related aspects. Support from strong leadership at the head of government level (OECD, 2015) is required so that cyber-security will be recognised as a critical government priority. According to the OECD (2015), most cyber-security strategies share the following key conceptions:

a. Improved government coordination at policy and operational levels. Cyber-security policy formulation, as a national government priority, can be implemented by being assigned within the government. It is important to note that no single vertical agency can have a sufficiently wide authority to manage all facets of cyber-security; also, no single agency can claim comprehensive understanding of cyber-security. This point emphasises the importance of coordination amongst relevant stakeholders.

b. Strengthened public–private cooperation is essential. Cyberspace is operated and owned by the private sector, to a large degree, and these users play an important role in the secure use of cyberspace.

2.3.4. The European Network of Information Security Agency (ENISA)

To address cyber-security threats, the European Union member states came together and formed the European Network of Information Security Agency (ENISA) which provides guidance on the formulation of a national cyber-security strategy. Key performance indicators are provided for each cyber-security strategy component. Through the *ENISA Guidebook*, a country's policy makers are guided by the practical recommendations for controlling the development and improvement process on national the cyber-security status and security affairs within the country (ENISA, 2015).

2.3.5. The African Union Convention on Cyber Crime and Personal Data Protection

In June 2014, the heads of member states of the African Union adopted the African Union Convention on Cyber Crime and Personal Data Protection. South Africa is an affiliated member state. This convention aims to harmonise the laws of African member states on electronic commerce, data protection, cyber-security governance and cybercrime control (Orji, 2018). The Convention also defines the objectives for the information society in Africa and seeks to strengthen existing ICT laws in member states. The convention mainly covers four areas which are the security of e-commerce, legal aspects, personal data protection, and cybersecurity (Ball, 2017). With regard to e-commerce, South Africa has the Electronic Communication, and Transactions (ECT) Act of 2002. For personal data protection, the country has Protection of Personal Information (POPI) Act of 2013.

The Convention has prescribed broad obligations for member states to establish national cyber-security policies as well as legal, regulatory and institutional frameworks for cyber-security governance and cybercrimes control. The Convention, in this regard, requires member states to implement obligations that include: establishing a national cyber-security framework; promoting a culture of cyber-security; establishing national cyber-security governance structures; protecting critical information infrastructure; establishing cybercrime offences and procedural measures; and, promoting international cooperation and legal harmonisation.

Member states are required to establish a national cyber-security framework that comprises a national cyber-security policy and a national cyber-security strategy. A member state’s national cyber-security policy is required to recognise the importance of national Critical Information Infrastructure (CII), and identify related risks using the all-hazards approach, while also outlining how the objectives of such a policy are to be achieved. The “all-hazards” approach to CII protection entails the protection of such infrastructure from all forms of threats, whether they originate from deliberate attacks, accidents or natural disasters. In addition, the obligation to establish a national cyber-security policy requires member states to outline how their national cyber-security policy will achieve the objectives of protecting national CII from identified risks. In 2015, South Africa published a National Cyber-security Policy Framework and has worked towards implementing the Convention’s requirements on cyber-security.

The Critical Infrastructure Protection Bill was tabled in Parliament on 15 September 2017. This Bill replaces the National Key Points Act (102 of 1980), and it deals with the process of the declaration of National Key Points. The Bill talks to the safeguarding of critical infrastructure and persons inside the critical infrastructure area. The Bill provides for the establishment of a National Infrastructure Council, and provides for designation and functions of inspectors, amongst others.

South Africa has made recognisable strides towards the legal aspect of cyber-security. The Government of South Africa published the Regulation of Interception of Communications and Provision of Communication-related information Act (RICA), 2002. The aim of RICA is to make the country safer as it assists law enforcement agencies to identify mobile phone users and track criminals using mobile phones for illegal activities. RICA regulates information communication interception and monitoring. On 9 December 2016, the Department of Justice and Correctional Services published the Cybercrimes and Cybersecurity Bill.

2.4. SOUTH AFRICAN NATIONAL CYBER-SECURITY POLICY FRAMEWORK (NCPF)

Cyber-security is one of the methods used to manage risks facing organisations, government and society. South Africa's National Security is heavily reliant on the security of critical infrastructure (Mahlobo, 2015). The National Critical Information Infrastructure plays a vital role in the maintenance of economic strength, public safety, public health, national image, defence and security, government capability to function, and other essential individual and public needs (Wamala, 2011). Facilities that are information-based, assets and networks such as water supply, electricity, finance, and many more, are essential to national infrastructure.

Cyberspace is the core to the provision of these national services (Wamala, 2011). Cyberspace has also become a national critical information infrastructure and, as such, its protection is of vital importance (ISO/IEC, 2012). The cyber-security landscape is increasingly evolving and, as a result, it is important for countries to manage the potential risk and vulnerabilities emanating from this situation (Wamala, 2011). One approach that countries can apply is to develop and implement policies, procedures and proactive strategies that are guided by a national cyber-security policy framework and strategy. The result of this locally was the signing and publishing of the *South African National Cyber-Security Policy Framework (NCPF)* in September 2015 by the Minister of State Security. The NCPF was developed in order to address and reduce the country's vulnerabilities and exposure to cyber-risks. National government leaders are accountable for cyber-security since governments, in the main, function to enable commerce, protect citizens' lives and property, and maintain social order.

Most efforts as guided by the NCPF are focused on promoting awareness, which is appropriate on its own; however, is insufficient (Grobler *et al.*, 2012). This research project advocates the approach of performing a rigorous quantitative risk assessment and utilising mitigation techniques. The central thrust is on cyber-security on national, provincial and local levels of government.

The NCPF of South Africa aims to promote a cyber-security culture by strengthening the judicial processes, including investigation, to ensure the safeguarding of the national critical information infrastructure. The aim is also to establish public-private partnerships for national and international plans of action, and to advance and ensure a comprehensive legal framework to govern cyberspace (ITU, 2015). In the main, the NCPF promotes the reduction of cyberspace vulnerabilities and cyber-threats and, most importantly, the prevention of attack, in the first instance. Where there is a cyber-attack, the policy needs to ensure a swift recovery of the critical information infrastructure (Mahlobo, 2015). The NCPF has acknowledged that currently there is no coordinated approach to dealing with cyber-security issues, despite having established various structures to deal with these issues (Phahlamohlaka, Jansen van Vuuren, & Coetzee, 2011). The development of cyber-security research is promoted by the NCPF in order to advance and enhance cyber-security research within South African tertiary institutions, industry and the Department of Science and Technology (Mahlobo, 2015). The NCPF aims to achieve the following benefits:

a. A cyberspace that is secure and safe and which underpins national security priorities.

b. A coordinated approach to addressing cyber-security through the establishment of institutional structures.

c. A national critical information infrastructure identification and protection framework.

d. Stimulation of economic growth and competitiveness of the country through a secure e-environment.

e. Advancement of cyber-security through the national research and development agenda.

f. Combating of cyber-crime through effective prevention and prosecution.

g. Improved cyber-security management.

2.5. CRITICAL INFORMATION INFRASTRUCTURE

The NCPF of South Africa defines the National Critical Information Infrastructure as all IT systems, such as databases, data systems, networks – including buildings – processes, people, and facilities that are essential to the effective functioning of the Republic (Mahlobo, 2015). There are various national and international definitions of CI where, in some countries, they stress the purpose of the infrastructure, whilst in others, they stress the effects of the destruction or disruption of infrastructure on society at large (Clemente, 2013). The Department of Homeland Security in the United States of America defines CI as “assets and systems, virtual or physical, so critical or vital to the nation such that the incapacitation or destruction of such assets and systems would have debilitating consequences on national security, economy, health and safety” (Clemente, 2013, p. 13).

CIs mostly perform their functions through the support of IT and industrial control systems and, as a consequence of this reliance on IT and ICS interconnectivity, there is increased potential of cyber-vulnerabilities and risk exposures. The municipalities' critical information infrastructure considerations entail the safeguarding and mitigation strategies of the critical systems, including both virtual and physical systems, and assets. Failure of these critical systems and assets would result in both economic and social unrest, if disrupted for a considerable amount of time (Dennis *et al.*, 2014). IT systems support and improve the services and information received from the municipalities' critical information infrastructures, the protection and security of which are municipal responsibilities and should therefore assume high priority. The list of municipalities' critical infrastructures includes: energy facilities like electricity; transmission and distribution systems; water SCADA systems; water reservoirs, treatment plants and networks; emergency services facilities; and transportation facilities, including traffic control systems, and ICT software and hardware, including the Internet infrastructure.

2.6. ATTACK ON CRITICAL INFRASTRUCTURE: THE STUXNET WORM

Stuxnet is a computer virus and was first discovered in July 2010 by Virus-BlockAda in Belarus (Chen, 2010). However, this worm had been around for several months and estimates around this vary. It has been estimated that Stuxnet has infected in the region of 50 000 to 100 000 computers, mainly in Iran, Indonesia, India and Pakistan (Chen, 2010). Stuxnet seems to be targeting the critical physical machinery of the intended organisation of which it attempts to take control. Stuxnet's final intention is to manipulate and reprogram ICS by making them function differently from their operator's or owner's intentions, and most probably outside their specified boundaries (Chen, 2010).

ICSs are operated on programmable logic controllers (PLCs) which are instructed by a specialised assembly-like code. Often the PLCs are programmed on Windows computers and are not connected to the Internet or even the organisational internal network (intranet). The attacker needs the ICS schematics for the intended target environment which are normally made available by insiders or through other reconnaissance methods (Falliere, Murchu, & Chien, 2011). Stuxnet may be introduced by a removable drive and once it infects a computer within the target environment, it begins to spread in search of PGs, which are used to program PLCs and are typically Windows computers (Falliere *et al.*, 2011). Once the Stuxnet finds a suitable intended computer, it modifies the PLC code and sabotages the

ICS. Stuxnet has the ability to conceal its modifications of the PLC; it attempts to isolate the rogue PLC code and this becomes a challenge (Chen, 2010).

Stuxnet developers are highly skilled software developers such that they have made it possible to compromise two digital certificates and inject malicious code into PLCs to affect the functioning of the ICS; furthermore, the code cannot be recognised by operators (Fallieres *et al*., 2011). Direct cyber-attacks on the CIs are not just a theory but a reality, and the Stuxnet Worm has proven that. It has been estimated that Stuxnet was developed by more than four people for over five months with access to SCADA systems (Chen, 2010) which shows the manpower required to develop this worm (Matrosov et al., 2010). The complexity and size of this worm – almost half a megabyte – is an indication that significant manpower was utilised in developing Stuxnet (Chen, 2010). The initial infection trajectory was a Universal Serial Bus (USB) and not the usual suspect Internet, and this is a clear indication that the cyber-attackers were familiar with the target environment and possibly knew that it was not reachable via the Internet (Chen, 2010).

To demonstrate the complexity and sophistication of Stuxnet, Karnouskos, (2011) highlighted that Stuxnet:

- used security gaps that the software coders/programmers were unaware of, such as zero-day exploits;
- was coded in way that revealed a function that was difficult and used a custom encryption algorithm for data configuration;
- used a stand-alone network, but was able to keep it posted automatically as the new version became available, and could keep in touch with all Stuxnet installations through peer-to-peer networks;
- ensured that no disk evidence existed since all actions were done in computer memory;
- disguised itself under legal programmes and could keep/record the number of infected machines – Stuxnet design architecture was modular, which is in line with the new trends in software development;
- could detect connectivity to the web and would attempt to connect to its commanders; it could also automatically deploy anti-virus detection mechanisms;

- would infect targeted systems in a unique manner and could lift up its rights in a computer that was unpatched through explicit exploits to have appropriate execution rights;
- would spread the virus to no more than three machines and had strict self-scalability control;
- had two inappropriately acquired digital certificates from separate organisations, which it used to deploy legal digitally-signed device drivers;
- could fake system process control sensor signals through the man-in-the-middle attack code; consequently, the relying processes and tools would falsely show normal boundaries' values and functionality that were not the real world representation;
- had a self-cycle management to delete itself on June-24-2012; and
- had externally configured websites as control and command servers to enable controlling and monitoring of functions; since most firewalls allow uploading of information from internal to external servers, there was industrial espionage taking place.

2.7. DIFFERENCES BETWEEN IT SECURITY AND CYBER-SECURITY

Safeguarding the industrial control systems is different from the safeguarding of IT systems when it comes to issues pertaining to cyber-security. It is, therefore, essential that the IT professionals and ICS professionals should work together to jointly develop a cyber-security solution that will benefit the entire municipality (Neitzel & Huba, 2014). According to Neitzel and Huba (2014), there are ten key differences between ICS and IT cyber-security and these are discussed below:

a. Security objective – The primary cyber-security objective for IT systems is to protect data (confidentiality). The main ICS cyber-security objective is to maintain the production process integrity and the availability of its components.

b. Network segmentation – Business IT systems are made of connected subnets that are connected to the Internet. Subsequently, protection from internet and access controls are IT networks security's primary focus. ICSs are seen as industrial intranets with two security needs, the first being that access to the Internet and e-mail is not permitted, and the second is that rigorous protection of ICS networks from other business networks is required, particularly those networks with access to the Internet. ICSs are isolated from other business IT networks through a ‘demilitarised’ zone (DMZ) which operates in-between the other business networks and the ICS.

c. Network topology – IT systems are often large and include Wi-Fi networks, data centres, and intranets. In contrast, ICSs are small and are composed of a configuration database and event/data historians. Normally IT systems comprise many nodes that are daily affected by the number of users and applications that are connected and disconnected continuously. On the other hand, the ICSs are considerably smaller and normally have configurations that are statically defined.

d. Functional partitioning – The functional partitioning of IT systems and ICSs are different. IT systems are commonly divided into different administrative partitions in order to restrict access to information. The partitioning of ICS is divided into three levels: Level 0, which represents the physical process; level 1, which is control and monitoring; and level 2, which is supervisory control. IT security cannot be mapped onto the ICS due to the fact that ICSs have vendor-specific security-related tools which are unknown to IT systems, such as universal serial bus ports disabling features, custom event logs, and port lockdown mechanisms.

e. Physical components – IT systems consist of off-the-shelf workstations, servers, and networks that IT can access and administer. Consequently, IT can define security policies for such components, and can implement off-the-shelf security-related tools such as anti-virus systems, firewalls, and patch management systems. ICSs are made up of components which are custom built and generally foreign to IT. These components include network devices for industrial use, such as Ethernet switches and firewalls, servers and workstations that are ‘hardened’ such that their software is custom built, and as a result, their security policies are industry standards which may not align with the ones used within IT systems.

f. User accounts – There are two types of user accounts in IT systems and these are the operating system user account, and the application-specific user account. ICSs have operating system user accounts and their own application-specific users that are role-based users to access controls for granting and denying access to control data and devices. Such roles include process engineers, operators, and maintenance engineers.

ICS is a complete distributed system that is made up of configuration, databases, event journals, operation, and maintenance applications.

g. Safety instrumented system (SIS) is a key aspect for ICS for the maintenance of the safe operation of the process, through putting into a safe state the process, when there is a detected condition that threatens the safety of the process. SISs are securely segmented and are separated from ICS networks. Therefore, managing the security of ICSs includes the safeguarding of SIS; all of these are normally not outside the IT systems professionals' scope.

h. Untested software – To maintain IT systems' security, it is critical to keep pace with the evolution of new software, thereby keeping the systems current. In contrast, ICSs are specific to hardware configuration and operating system versions, and, when the component is changed or updated, other components may not run appropriately. Thorough testing of patches and virus definition files must happen first, before approval is given for implementation. IT systems' new software is often not rigorously tested for compatibility with the IT system.

i. Patching – IT systems, generally, have software for managing patching to automatically and quickly install security updates. ICS patching takes a longer time because those patches require testing, approving, scheduling and validating to maintain the state and to render control repeatable.

j. Security inconveniences – Security measures that are tolerable for IT systems are intolerable for ICS. For example, in IT systems the users have to wait for the operating system's patches update to finish before using the system, and wait for the helpdesk to reset the user control password. These inconveniences are intolerable in ICS due to the criticality of services provided by the ICS systems. Consequently, the security measures that are acceptable in IT systems may not necessarily be the same for ICSs. If IT systems' security measures are enforced indiscriminately, they may pose a serious threat to ICS security.

2.8. CURRENT RESEARCH PERSPECTIVES ON CYBER-SECURITY IN SOUTH AFRICA

2.8.1. National cyber-security in South Africa

Like the rest of the world, South Africa has become increasingly reliant on cyberspace to conduct business and to govern. This reliance has increasingly exposed the country to threats that are inherent in cyberspace (Von Solms & Von Solms, 2015). South Africa approved a cyber-security policy in March 2012; however, there is no reported progress towards the implementation thereof (Von Solms & Von Solms, 2015). Other countries are reporting progress they have made towards safeguarding their cyberspace, which is regarded as the essential requirement for contemporary critical information infrastructure, society and the economy. South Africa has released its national cyber-security policy framework, which highlights the need to have a coordinated approach to addressing cyber-security issues. National government is responsible for this coordination, but various institutions within the country are the owners and custodians of national critical information infrastructures. The country needs to act urgently on the implementation of cyber-security strategies (Von Solms & Von Solms, 2015) as it cannot continue to drag its feet on protecting our cyberspace. The national cyber-security policy framework identifies what the country aims to implement towards addressing the protection of cyberspace. The framework needs to be followed by generating strategy documents that will address related cyber-security issues, and these strategy documents need to spell out clearly how the country intends to address cyber-security (Von Solms & Von Solms, 2015). Various countries have spent and are still spending huge budgets on the implementation of their cyber-security-related strategies, and some have even considered quality control mechanisms in the strategy itself and in the implementation thereof (Von Solms & Von Solms, 2015).

2.8.2. Fostering a cyber-security culture: A case of South Africa

South Africa is currently one of the leading countries when it comes to knowledge of cyber-crime matters (Kortjan & Von Solms, 2014), and this may be attributable to the recent bandwidth increase. Taking into cognisance all that has happened in the country regarding cyberspace crime, and South Africa's exposure to the possibly devastating consequences of cyber-ills, cyber-security efforts have not been matching the pace set by innovations related to cyberspace usage, according to Kortjan and Von Solms (2014). Their research is meant to address the inadequate emphasis on cyber-security education in the country. A cyber-security culture is necessary to inculcate acceptable user behaviour in cyberspace. The increasing dependence on cyberspace and digital resources has, unintentionally, invited many exposures to malicious cyberspace attacks. South Africa aims to promote a cyber-security culture which is envisaged to advance the national cyber-security policy framework; however, there is no discussion on how this cyber-security culture will be promoted. According to the research in question, awareness and education are regarded as pillars in promoting a cyber-security culture (Kortjan & Von Solms, 2014) and it is argued that appropriate awareness campaigns would aid in fostering the desired cyber-security culture. It is highlighted that comprehensive awareness initiatives could impact positively on changing the behaviour of cyberspace users towards a cyber-secure culture (Kortjan & Von Solms, 2014).

2.8.3. Cyber-security awareness initiatives in South Africa: A synergy approach

One of the top cyber-crime types reported in South Africa is phishing attacks and the country is one of the top three countries facing this threat, behind only the UK and US (Dlamini & Modise, 2013). It is argued that the existing approach to promoting cyber-security awareness is not making an adequate impact, especially because of the uncoordinated and fragmented nature of the approaches (Dlamini & Modise, 2013). It is acknowledged, however, that cyber-security is multi-faceted and complex. The estimated total cost of cyber-crime in South Africa is R10.9 billion, which is one per cent of the R2.9 trillion of global cost (Dlamini & Modise, 2013). Their research suggests that the first line of defence against cyber-attack is cyber-security awareness.

Their study also highlights the fact that, in South Africa, initiatives that are intended for cyber-security awareness are delivered via various independent mechanisms that are uncoordinated. Cyber-security awareness is intended to promote and inspire cyberspace users to practise safety precautions when using cyberspace. Users should be kept well informed on the criticality of practising cyberspace hygiene at all times; hence the awareness initiatives should include a plan that is clear, with goals and objectives clearly articulated and the targeted results clearly stipulated (Dlamini & Modise, 2013). Their research indicates that the cyber-security initiatives in the country are effective, although these initiatives are on a smaller scale than they should be. These initiatives are reported to be comparable with counterparts internationally and their focus is on communities. A recommendation is made that a single forum to integrate a cyber-security awareness mechanism be formulated to ascertain whether all necessary roles and key players of each initiative are spelt out clearly, and that these awareness programmes reach every cyberspace population in the country.

2.8.4. An e-safety educational framework in South Africa

This study highlights the concern around the safety of children in cyberspace (De Lange & Von Solms, 2012). IT has an important role to play in human lives, but the benefits it brings also expose individuals to risks. The research argues that IT threats should be taught to children at a young age and that children need to be educated on acceptable online behaviour. They also need to be educated on cyber-bullying and illegal or inappropriate online behaviour. Currently, there appears to be a generational divide between parents and their children and many parents are unaware of both cyber-ills and of activities being conducted by their children online. E-safety is considered essential and should be implemented to protect the lives of children.

Most countries have introduced e-safety in their curricula; however, South Africa is lagging behind in terms of e-safety implementation. E-safety awareness in the country is lacking and should be viewed seriously by the government. Their study acknowledges that the implementation of e-safety at schools will inculcate the desired cyber-security culture in the entire population.

2.8.5. Implementation of the NCPF for South Africa

Volatility and dynamicity of cyberspace warrant robust research in the area of cyber-security in South Africa (Van Vuuren, Leenen, & Zaaiman, 2014). In order for South Africa to safeguard its resources and population, the country needs to protect its critical infrastructure, especially as it relates to national security. The South African geographical regions are incorporated into the global cyberspace, warranting government's extra efforts at addressing the digital divide and cyber-security. Cyber-security has been identified as a basic essential element contributing towards national security with critical information infrastructures and information itself being essential in the implementation and roll-out of a cyber-security policy. Government has a critical responsibility to enhance and advance cyber-security awareness campaigns, particularly because the entire nation is hugely dependent on essential services that are rendered by government. The process of developing the national cyber-security policy framework has taken far too long, but the policy framework has since been finalised. Van Vuuren *et al.* (2014) argued that there is no adequate emphasis on the national cyber-security policy, despite the fact that such a policy would be an overarching document to guide the cyber-security implementation in the country. In an effort to safeguard the cyberspace, this research proposes an ontology that identifies various stakeholders and defines their roles. It has been recognised that a multi-levelled structure of key stakeholders exists in the cyber-security environment and that, more often than not, the responsibilities and roles overlap.

2.9. SOUTH AFRICAN CYBER-SECURITY STATISTICS

As part of the Global Forum for Cyber Expertise initiative, the African Union Commission and Symantec in 2016 released a report on the cyber-crime and cyber-security trends in Africa. The report highlights the increase of technology adoption in Africa. It further posits that policymakers need to stem the cyber-security rising tide through the implementation of effective policies and awareness initiatives (Symantec, 2016b). The report provides the following statistics:

a) 67% of South Africans have experienced some form of online crime compared to 48% globally.

b) 20% of South African social network users share their passwords with others, while 21% connect with people they do not know.

c) 67% of adults reported experiencing cyber-crime is estimated to have cost the South African economy $242 million USD.

The report (Symantec, 2016b, p. 89) provides the following significant crimes that are associated with cyber:

- **"Gautrain incident:** Computer-related theft/fraud committed by a group of persons. There was insider collusion with IT persons working for company. Value of potential loss was in the region of R800 Million.
- **Eskom incident:** Attempted computer-related theft/fraud committed by a group of persons. There was insider collusion with IT persons working for company. Value of potential loss was in the region of potential loss R3.5 Billion.
- **Telesure incident:** Relates to ransomware. Potential loss in the region of R20 Million. Perpetrated by a group of persons".

The picture that is clearly articulated in the report relates to the lack of necessary capacity to systematically implement cyber-security strategy in the country. The report states that "the biggest impediments is probably the slow pace at which the NCPF is implemented and the unavailability of resources and capacity" (Symantec, 2016b, p. 88). The report argues that in order to ensure capacity building, government should promote special initiatives. It further put a stance that when implementing the NCPF, an incremental approach is adopted, which entails focusing on aspects that require to be attended to urgently.

The report lists the following tables which present the top ten source (originating from) African countries for malicious behaviour and their percentages within the continent.

a. Attacks

"Attackers use various exploits to gain unauthorized access to a computer or an organization's network. Motivations for these attacks can range from gaining financial profit, stealing sensitive information, disabling a network, establishing a C&C server, or using the system as a launching point for future attacks. Attacks can be active such as a brute-force attack that determines a user's password, or passive such as a web-based attack that waits for a user to visit a malicious webpage in an attempt to infect the user's computer with malicious code" (Symantec, 2016b, p. 31).

Table 2.3: Top ten malicious attacks

Country	Rank	Percentage within Africa	Incident count
South Africa	1	25%	314,880
Egypt	2	12%	149,685
Kenya	3	9%	106,265
Nigeria	4	7%	89,100
Mauritius	5	6%	73,134
Algeria	6	5%	60,381
Seychelles	7	4%	45,661
Botswana	8	3%	37,880
Morocco	9	3%	34,464
Tunisia	10	3%	32,187

Source: Symantec. (2016b). *Cyber-crime & cyber security*, p. 25. [Online] Available WWW: https://www.thehaguesecuritydelta.com/media/com_hsd/report/135/document/-Cyber-security-trends-report-Africa-en.pdf.

b. Malware

"Malware is software that attackers use to steal confidential information, destroy data, disrupt computer operations, or gain access to the network from the compromised system. Types of malware include viruses, worms, Trojans, and ransomware, and they spread through the use of a variety of tools such as e-mail, drive-by downloads, and infected files. They can also exploit existing vulnerabilities to infect systems" (Symantec, 2016b, p.35).

Table 2.4: Top ten malware sources

Country	Rank	Percentage within Africa	Incident count
South Africa	1	20%	1,716,308
Tunisia	2	14%	1,166,774
Kenya	3	8%	668,194
Nigeria	4	6%	469,018
Cote D'Ivoire	5	5%	407,112
Ghana	6	5%	405,805
Egypt	7	5%	400,679
Algeria	8	4%	304,114
Ethiopia	9	3%	245,172
Cameroon	10	3%	224,546

Source: Symantec. (2016b). *Cyber-crime & cyber security*, p. 26. [Online] Available WWW: https://www.thehaguesecuritydelta.com/media/com_hsd/report/135/document/-Cyber-security-trends-report-Africa-en.pdf.

c. Spam

Spam is an **unspecified, unsolicited bulk e-mail** which eats up a lot of network bandwidth, and is sent in huge quantities using deceived sender addresses to conceal the real sender. Examples of spam can include advertising materials and newsletters if the receiver did not elect to receive it.

Table 2.5: Top ten spam sources

Country	Rank	Percentage within Africa	Incident count
South Africa	1	24%	271,700,021
Tunisia	2	14%	160,301,789
Egypt	3	7%	78,429,009
Kenya	4	7%	78,410,109
Nigeria	5	4%	50,491,804
Algeria	6	4%	50,253,534
Cote D'Ivoire	7	4%	47,632,285
Ghana	8	4%	43,938,441
Morocco	9	3%	32,197,294
Cameroon	10	2%	25,478,566

Source: Symantec-1. (2016b). *Cyber-crime & cyber security*, p. 27. [Online] Available WWW: https://www.thehaguesecuritydelta.com/media/com_hsd/report/135/document/-Cyber-security-trends-report-Africa-en.pdf.

d. Phishing hosts

Phishing is when an attacker deceives a person, mainly through e-mail communication to distribute mischievous attachments or links that can achieve a variety of purposes, including the extraction of user profile or credentials.

Table 2.6: Top ten phishing host sources

Country	Rank	Percentage within Africa	Incident count
South Africa	1	74%	4,621
Morocco	2	5%	319
Egypt	3	3%	184
Kenya	4	3%	160
Nigeria	5	2%	136
Tunisia	6	2%	112
Cameroon	7	1%	57
Libya	8	1%	53
Zimbabwe	9	1%	51
Algeria	10	1%	48

Source: Symantec-1. (2016b). *Cyber-crime & cyber security*, p. 28. [Online] Available WWW: https://www.thehaguesecuritydelta.com/media/com_hsd/report/135/document/-Cyber-security-trends-report-Africa-en.pdf.

Cyber-security efforts in South Africa are led by the Cyber Response Committee which operates under the State Security Agency's oversight (Symantec, 2016b). This interim committee has the following role players:

a) South African Police Service (SAPS), which plays the role relating to the investigation of cybercrimes.

b) Department of Telecommunication and Postal Services is the custodian of a cyber hub, and supports initiatives to ICT users on cyber-security matters.

c) Department of Justice and Constitutional Development whose role is legislation drafting.

d) State Security Agency provides administration support to the Cyber Response Committee and is also responsible for the implementation of cyber-security initiatives in the country whilst waiting for promotion of comprehensive legislation on various aspects of cyber-security.

e) Department of Science and Technology plays a significant role in the development and implementation of research and initiatives to advance the needed skills to deal with cyber aspects in the country.

f) Department of International Relations and Cooperation, which is responsible for international relations specific to cyber-security.

g) Department of Defence is responsible for the cyber offensive and defensive development and implementation thereof.

2.10. LOCAL GOVERNMENT LEGISLATIVE FRAMEWORK IN SOUTH AFRICA

This section discusses the pertinent local government legislation that is important to the objectives of this enquiry which aims to assess the cyber-security status of metropolitan municipalities in South Africa.

2.10.1. Constitution of the Republic of South Africa

The Constitution (RSA, 1996) is the supreme law of the Country. No other Act or legislation in South Africa can override the prescription of the Constitution. Chapter seven (7) of the Constitution is dedicated to the local government in the country. Section 151 of the Constitution provides the status of municipalities and states that: "(1) The local sphere of government consists of municipalities, which must be established for the whole of the territory of the Republic; (2) The executive and legislative authority of a municipality is vested in its municipal council; (3) A municipality has the right to govern, on its own initiative, the local government affairs of its community, subject to national and provincial legislation, as provided for in the Constitution, and (4) The national or a provincial government may not compromise or impede a municipality's ability or right to exercise its powers or perform its functions" (RSA, 1996).

Municipal responsibilities are presented in section 152 which states that "(1) the objects of local government are-

(a) *To provide democratic and accountable government for local communities;*
(b) *To ensure the provision of services to communities in a sustainable manner;*
(c) *To promote social and economic development;*
(d) *To promote a safe and healthy environment; and*
(e) *To encourage the involvement of communities and community organisations in the matters of local government"*

Section 155 of the constitution makes provision for the establishment of municipalities under the following categories. It states:

"(a) ***Category A:*** *A municipality that has exclusive municipal executive and legislative authority in its area.*
(b) ***Category B:*** *A municipality that shares municipal executive and legislative authority in its area with a category C municipality within whose area it falls.*
(c) ***Category C: A*** *municipality that has municipal executive and legislative authority in an area that includes more than one municipality".*

2.10.2. The Municipal Finance Management Act, No.56 of 2003

National Treasury introduced financial management reforms across government in 1994 and in local government in 1996. The Municipal Finance Management Act (MFMA) is the cornerstone of the local government reform, and seeks to provide a framework for financial management to maximise municipalities' capacity to deliver services as entrenched in the

Constitution (RSA, 2003). This act intends to establish a sound financial governance framework by describing roles and responsibilities of officials, the Mayor, and Council. Cyber-security initiatives are dependent on the management support which could include financial support. The financial support ought to fall under the ambits of MFMA. The prescripts of MFMA must be met including budgeting requirements if management is to provide financial support to implement cyber-security processes in the municipality.

2.10.3. Municipal Systems Act, no 32 of 2000 (MSA)

The Municipal Systems Act (MSA) (RSA, 2000) states that "A municipality-

(a) *is an organ of state within the local sphere of government exercising legislative and executive authority within an area determined in terms of the Local Government: Municipal Demarcation Act, 1998;*

(b) *consists of-*

(i) *the political structures and administration of the municipality; and*

(ii) *the community of the municipality;*

(c) *functions in its area in accordance with the political, statutory and other relationships between its political structures, political office bearers and administration and its community; and*

(d) *has a separate legal personality which excludes liability on the part of its community for the actions of the municipality".*

One of the objectives of the act is to ensure universal access to essential services (RSA, 2000). The MSA refers to basic municipal services as "a municipal service that is necessary to ensure an acceptable and reasonable quality of life and, if not provided, would endanger public health or safety or the environment" (p, 14). Cyber-security breaches can be one of the serious risks that can negatively impact the municipality to deliver some of such basis services. Section 4 (2)(a) of MSA Chapter 2 prescribes that "the council of a municipality, within the municipality's financial and administrative capacity and having regard to practical considerations, has the duty to exercise the municipality's executive and legislative authority and use the resources of the municipality in the best interests of the local community" (RSA, 2000).

2.10.4. Local government: Municipal Structures Act 117 of 1998

The Structures Act prescribes the municipalities in the country to develop an Integrated Development Plan (IDP) which is a strategic plan document for municipalities (RSA, 1998). Section 26 of the Structures Act presents components that must be contained in an IDP document and it states that "An integrated development plan must reflect *(a)* the municipal council's vision for the long term development of the municipality with special emphasis on the municipality's most critical development and internal transformation needs; *(b)* an assessment of the existing level of development in the municipality, which must include an identification of communities which do not have access to basic municipal services; *(f)* the council's operational strategies; *(g)* applicable disaster management plans; *(h)* a financial plan, which must include a budget projection for at least the next three years". Cyber-security initiatives within the municipality are part of Council's operational strategies. Financial support should be incorporated into the financial plan as prescribed by the Structures Act applied together with the MFMA.

2.10.5. Definition of a metropolitan municipality in South Africa

The Structures Act (RSA, 1998) defines Category A Municipality (Metropolitan Municipality) as

"(a) a conurbation featuring—

(i) areas of high population density

(ii) an intense movement of people, goods, and services:

(iii) extensive development: and

(iv] multiple business districts and industrial areas; ~o

(b) a centre of economic activity with a complex and diverse economy:

(c) a single area for which integrated development planning is desirable: and

(d) having strong interdependent social and economic linkages between its constituent units".

2.11. CHAPTER SUMMARY

The chapter presented a review of literature that was considered pertinent for this study. Globally, various governments have different views on cyber-security, but all those views converge around protecting resources/assets that are impacted by cyberspace risks. Various international organisations have developed standards/guides/frameworks that member countries should adopt for addressing cyber-security matters. The RSA NCPF was discussed. Cyber-attacks on PCS was discussed, and an example of such attacks was the Stuxnet Worm. The chapter highlighted the differences between IT security and cyber-security. Various research perspectives on cyber-security in the context of South Africa were discussed. Finally, the RSA legal framework on local governments was discussed where the Constitution, MFMA, MSA, and the structures Act were presented. A definition was provided of a metropolitan municipality from the context of the Structures Act (RSA, 1998).

CHAPTER 3
RESEARCH DESIGN AND METHODOLOGY

3.1. CHAPTER INTRODUCTION

The chapter presents the philosophical worldviews and research methodology that were adopted for this research. The sections discussed are presented in Table 3.1.

Table 3.1: Structure of Chapter 3

	Topic	**Overview**
3.1	Chapter introduction	Provides context and road map of the chapter.
3.2	Philosophical worldviews	Discusses research paradigms.
3.3	Justification for choosing constructivist worldview	Researcher's stance on adopted paradigm.
3.4	Grounded theory methodology	Presents research method adopted in the enquiry.
3.5	Study population	Discusses the profile of participants to the study.
3.6	Data collection	Presents enquiry's data collection methods.
3.7	Theoretical sampling	Discusses how the participants were chosen.
3.8	Data analysis	Presents data analysis techniques adopted.
3.9	Credibility, originality, resonance and usefulness	Discusses guidelines adopted to achieve credibility.
3.10	Grounded theory guidelines for IS studies	Discusses GT guidelines for IS studies considered.
3.11	Chapter summary	Presents highlights on the topics covered in the chapter.

Constructivism was the chosen worldview for this research. The other worldviews are also discussed, particularly positivism and pragmatism. The chapter also highlights how the chosen research methodology guided data collection, data analysis and theory development. Amongst the various GTM approaches, the constructivist GT of Charmaz (2006) was the adopted approach for this investigation.

3.2. PHILOSOPHICAL WORLDVIEWS

In academic research, the research is predisposed by the researcher's worldview known as the paradigm. The researcher's belief system is a position of fundamental viewpoint pertaining to (a) the nature of the world; (b) the person's position in it; and (c) the extent of relationships possible to that world (Guba & Lincoln, 1994). Academic research is underpinned by theoretical assumptions about what constitutes valid research and appropriate research methods for the development of knowledge (Klein & Myers, 1999). The research process has three dimensions: ontology, epistemology and methodology. These three dimensions define the nature of enquiry (Terre Blanche, Durrheim, & Painter, 2006) through an all-encompassing system of interrelated practice and thinking called a research paradigm. Ontology relates to the nature of reality, epistemology refers to how one knows what one knows, and methodology relates to the modus operandi or mode of operation used in one's research. The research paradigm guides how knowledge is processed and how values and reality are interpreted. A paradigm is a set of values, beliefs and assumptions regarding the nature and conduct of research. Sometimes a paradigm in a research process is referred to as a worldview (Creswell J. W., Research design: Qaulitative, Quantitative, and Mixed Method Approaches, 2009).

The research methodology is a process followed by the researcher to execute the research process. The questions that the researcher poses in the research and the approach used to find solutions to those questions are influenced by the worldview of the researcher (Morgan, 2007). Traditionally, a researcher is influenced by either a positivist (quantitative) worldview or a constructivist (qualitative) worldview (Crotty, 1998). Pragmatists argue that research always happens in social, historical, political and other settings or contexts (Creswell, 2013). However, this research employed a constructivist worldview as the lack of cyber-security research in the context of local government in South Africa requires a more holistic approach.

3.2.1. Positivist/post-positivist worldview

Positivists argue that there is a single reality and aim to identify causal relationships through objective quantitative measurements. This worldview gives rise to a research approach that is sometimes referred to as the scientific method (Creswell J. W., 2013). Positivists approach research by examining the relationships among variables (Creswell J. W., 2013). The researcher is independent to avoid bias in the process of inquiry. Positivists develop knowledge based on observation and measurement of the objective reality that exists in the world. In this worldview, researchers argue that there are laws or theories that govern the world. These laws and theories need to be verified in order to understand the world

(Creswell, 2013). The conventional research approach in this worldview is that the researcher starts with a theory, then collects data to support or refute the theory, then designs tests and executes necessary revisions (Creswell, 2013). The research aims to construct relevant, true statements that can serve to explain the situation of concern. An essential aspect of competent inquiry is being objective; hence validity and reliability are critical in this worldview.

3.2.2. Constructivist worldview

Constructivists contend that there are multiple realities and different interpretations which are shaped by particular circumstances in the process of inquiry. The researcher is thus subjective in constructivism. A qualitative researcher follows an approach for exploring and understanding the meanings people ascribe to a social problem (Kaplan & Maxwell, 2005). The constructivist research approach entails emerging questions, data collection in the interviewee's setting, inductively building from particulars of general themes, and interpreting the data meanings (Creswell J. W., 2013). Such researchers inductively develop or generate a theory or pattern of meaning. This worldview posits that human beings develop meanings as they interact with the world on the basis of their social perspectives (Kaplan & Maxwell, 2005). By visiting the environment of the interviewees and collecting information personally, the researcher aims to understand the setting (Crotty, 1998).

3.2.3. Pragmatic worldview

Pragmatists argue that inquiry always take place in social, historical, political and other settings or situations (Creswell, 2013). As the name implies, the researcher foregrounds practicality and efficacy in their approach. The researcher draws from both qualitative and quantitative assumptions when conducting the research; the researcher focuses on the research problem instead of focusing on any one method, hence the use of all available approaches in order to understand it (Cherryholmes, 1992). Having a pragmatic worldview opens the door for mixed method researchers to use multiple methods, different assumptions, different worldviews and various forms of data collection and analysis (Morgan, 2007). The pragmatic worldview, therefore, gives rise to mixed methods research as the inquirer has freedom to select the methods that best meet the purpose of the research. Consequently, researchers employ both qualitative and quantitative data since they are useful in understanding the study problem (Morgan, 2007).

3.3. JUSTIFICATION FOR CHOOSING CONSTRUCTIVIST WORLDVIEW

In executing the study, the researcher aims to develop theory through the process of data collection from the real context. The researcher intends to follow an approach for exploring and understanding the meanings people ascribe to a social problem; and, in the case of this study, evaluating cyber-security status in the metropolitan municipalities in South Africa. This study sought to inductively generate a theory or pattern of meaning through the continuous collection of empirical data from the research participants. Combination of GT and a constructivist approach allowed analysis and interpretation of the participants' perspectives through the identification of concepts and categories from collected empirical data.

3.4. GROUNDED THEORY METHODOLOGY (GTM)

Barney Glaser and Anselm Strauss (1967) are the originators of the GTM. They argued that through qualitative data analysis, theory could emerge (Glaser & Strauss, 1967). GTM was developed for health and medical sociology research domains (Charmaz, 2006). Over the years, the application of GTM has gradually extended to other areas such as IS (Lehmann, 2010). For emergent research areas such as the cyber-security environment, GT is regarded as the 'best fit' method as it guides conceptual foundations that are grounded in empirically collected data. Theory development that is grounded in data during concurrent data collection and analysis technique is a tenet for GTM (Charmaz, 2008). GT was proposed by Glaser and Strauss (1967) as a four-step methodology from which theory emerges from data. The first step entails data coding by means of assigning unique identifiers (codes). The second step entails bringing together the codes with similarities in concepts to form categories. The third step brings together the categories based on their relationships to create a substantive theory. The forth step employs the substantive theory that emerged from the previous step to explain the phenomenon.

For IS research, the relevance of GT includes its ability to interpret multifaceted phenomena, social issues accommodation, its appropriateness for socially constructed experiences, and its absence from the limitations of prior knowledge (Glaser & Strauss, 1967). It is for this reason that the GTM was chosen for this research. The complexity and multifaceted nature of the IS environment requires a full conceptual understanding of wrestling with many interwoven and overlapping themes (Walsham, 1995). GT, as an interpretive approach to research, provides thick descriptions which help to disentangle conceptual relevance

(Fernandez, Lehmann, & Underwood, 2002). The value that is derived from this is the meaningful emergent concepts (Charmaz, 2006). Practitioners in the IS environment are preoccupied with issues that are of a socio-technical nature.

The three prominent schools of thought of GTM are: Charmaz constructivist, Classic – also called Glaserian, and Straussian grounded theory. The following table presents the characteristics of each view.

Table 3.2: Characteristics of prominent GTM

		Constructivist	**Straussian**	**Glaserian**
1	Worldview	Constructivism	Post-positivism	Positivism
2	Study problem identification	• Sensitisation of the concepts • Experience	• Literature • Pragmatism • Experience	No need to depend on literature review in the beginning
3	Relationship with participants	Co-construction	Active	Independent
4	Investigation & theory development	Co-construction & reconstruction of data toward theory	Paradigmatic checking model	Emphasis on the emergence of data through the induction process
5	Data collection	Emphasis on intensive interviews	Emphasis on observation, analysis of documents, interviews, and videos	Emphasis on interviews and observation
6	Data analysis	• Initial coding • Focused coding	• Open coding • Axial coding • Selective coding	• Open coding • Selective coding • Theoretical coding
7	Memoing & diagrams	Flexible	Valuation of diagrams and memos	Intensification in the use of memos
8	Theory evaluation	• Congruence & consistency of the theory in relation to the context • Reflective interpretation of the researcher	• Adjustment • Theoretical generalisation • Control	• Applicability • Operability • Relevance • Changeability

Classic and Straussian are associated with the positivist view that theory is not formulated through the predetermined assumptions of researchers but is entrenched in the research data collected. On the other side, the Charmaz (2006) constructivist grounded theory is built on the premise that researchers should construct theory on the foundation of their "past and present involvements and interactions with people, perspectives, and research practices" (Charmaz, 2006, p. 19) and present an understanding of what is studied. Various schools of thoughts of GTM have different attributes. Therefore it is important for the researcher to make known the specific perspective applied in the study.

3.4.1. Classic grounded theory methodology overview

Classic grounded theory methodology originates from the Glaser and Strauss stance that research conducted for theory development purposes should be on an equivalent traction with studies executed to verify theory. Relative to theory generation, Glaser and Strauss (1967) posited that researchers have not "focused directly on how their theory emerged; as a result, they have not explored how they could have generated more of it more systematically, and with more conceptual generality and scope" (Glaser & Strauss, 1967, p. 27). Glaser and Strauss (1967) put theory as an evolving process that is "an ever-developing entity" and not a "perfect product" (Glaser & Strauss, 1967, p. 32). In formulating a theory, there is the constant comparative method which is a process by which theory unfolds through constantly selecting the data as it is collected. Glaser and Strauss (1967) highlighted the following four stages to the constant comparative method:

- Categories are matched to the incident or accounts. In this situation, the enquirer looks for connections and differences in how the categories are articulated in the data that has been collected.
- Linking properties to categories. In this situation, the enquirer develops ideas about the categories and their properties that may eventually arise from the collected data. This is achieved through a memoing process.
- Delineating the grounded theory. In this instance the researcher begins to make an intellectual association between categories and properties.
- Formulating substantive theory. This is the constant comparative method final phase.

To the fundamental spirit of GT, Glaser (1992) viewed it absurd to begin with a theoretical standpoint before conducting research. To begin with a preconceived theoretical perspective results in the substantive theory being biased (Glaser, 1992). The implication of the Classic GT perspective is that the literature review process is postponed to the end, after a theory has been generated. Glaser (1992) contended that interviewees would tell the researcher their main concern and the resolution strategy in a particular setting, and hence the main focus is on what emerges in the setting without the involvement of the researcher, and preconceived theoretical underpinning. During the data analysis process, Glaser (1992) relied on theoretical codes working on the tensions between theoretical sensitivity and extant theoretical concepts. The theoretical codes introduced by Glaser (1978) include theoretical families of concepts such as "Six Cs: Causes, Contexts, Contingencies, Consequences, Covariances, and Conditions" (Glaser, 1978, p. 74). Charmaz (2008) argued that coding families in some instances are arbitrary and haphazard as inevitably they are not mutually exclusive. Classic, Straussian, and Constructivist all prefer purposive and theoretical sampling strategies. Glaser (2004) lumped all non-classic grounded theory methodologies into what he referred to as "remodelled" grounded theory (Glaser, 2004).

3.4.2. Straussian grounded theory methodology overview

Classic grounded theorists discard any prior knowledge they possess on the focus of their research. As grounded theorists, Strauss and Corbin (1998) stated whether "we want to admit it or not, we cannot completely divorce ourselves from who we are or what we know. The theories we carry within our heads inform our research in multiple ways, even if we use them quite un-self-consciously" (Strauss & Corbin, 1998, p. 47) and consequently, that is a departure of Straussian grounded theory from classic grounded theory. Both Straussian and Classic grounded theories as methodological similarities adopt the constant comparative method, purposive and theoretical sampling techniques.

The main difference between the Straussian and Classic grounded theorists is at the data analysis processes. Strauss (1987) viewed induction, deduction and verification as forming important aspects of data analysis and he stated they are "absolutely essential" (Strauss, 1987, p. 12). On the other hand, Glaser viewed GT as inductive only. Strauss put emphasis on deduction and verification, and hinted about the overstated role of induction by the Classic grounded theorists.

Compared to Glaser, Strauss and Corbin (1990) put less emphasis on the emergence of what is happening in the setting but indicated that it is preferable to start from a wider lens. They contended that in addition to what emerges from the happening in the setting, professional necessities, personal experiences, and other influence may spark the research (Strauss & Corbin, 1990). Strauss's perspective on the emergence includes interaction, construction and reconstruction of meaning. In their data analysis technique, they applied axial coding and the causal conditional matrix, particularly as a means of specifying category dimensions, delineating relationships between categories into a coherent whole account. This data analysis approach is essentially a different technique from that of Glaser.

3.4.3. Constructivist grounded theory overview

This study adopted the constructivist grounded theory. This school of thought assumes that the enquirer's experiences, prior knowledge of relevant theory and values will surface in the grounded theory that develops from the enquiry. Predominantly, ConGTM "explicitly assumes that any theoretical rendering offers an interpretive portrayal of the studied world, not an exact picture of it" (Charmaz, 2006, p. 10). Both the researcher and the participants participate in formulating the theory. By following the constructivist grounded theory, the researcher has a chance to voice their point of view while at the same time allowing the interviewees' voices to be heard.

"Grounded theorists' background assumptions and disciplinary perspective alert them to look for certain possibilities" (Charmaz, 2006, p.16). Charmaz (2006) put supreme importance on richness of data rather than quantity. She adopted a coding protocol for data reduction similar to the coding process first proposed by Glaser and Strauss (1967), but attached different labels to the coding phases. For instance, Charmaz (2006) referred to open coding as initial coding, after which she applied a focused coding strategy. Initial coding entails comparing incidents or line by line, word by word, or paragraph by paragraph. "Focused coding requires decisions about which initial codes make the most analytic sense to categorise your data inclusively and completely" (Charmaz, 2006, p. 57). Focused coding or selective coding allows the researcher to classify and synthesize large amounts of data. Focused codes are scrutinised to assess which ones best explain or interpret the empirical phenomenon. Focused codes through an emergent process, are tested against the data. Researchers look for those codes that carry the weight of the analysis to become tentative theoretical categories.

Charmaz (2006) alluded to the fact that it is essential to understand the question of what theory is before embarking on a grounded theory study. Charmaz (2006) "calls for the imaginative understanding of the studied phenomenon... [and] assumes emergent, multiple realities; indeterminacy; facts and values as linked; truth as provisional; and social life as processual" (Charmaz, 2006, p. 126). Charmaz (2006) argued that theory emerges from the shared relationship of the researcher and participant, both being influenced by their prior values, beliefs and experiences. Further, Charmaz (2006) claimed that regardless of the theoretical perspective, theories are rhetorical in that they function to "present arguments about the world and relationships within it, despite sometimes being cleansed of context and reduced to seemingly neutral statements" (Charmaz, 2006, p. 128).

Charmaz (2006) also argued that the approach to enquiry followed by grounded theorists should offer a systematic inductive, comparative, and interactive format which offers several open-ended strategies for conducting emergent inquiry. These strategies provide more than the inductive only as they encourage the interviewer to make inferences, check them through engaging in deductive reasoning as the research progresses. These strategies make the grounded theory method explicit, and the development of emergent conceptual analysis is fostered by their open-ended qualities.

Theory emergence has elements of subjectivity emanating from collectively agreed-upon objective properties. In the beginning of GT, the researcher moves from inductive logic through to abductive reasoning. The application of abductive reasoning seeks to accommodate anomalies, and surprises in the collected data. With regard to emergence, the constructivist grounded theorist's position differs from both Glaser's (1978) theoretical codes and Strauss and Corbin's axial coding together with a conditional matrix. The argument is that both approaches promote researchers to force their data into extant categories. The constructivist grounded theorist sees theoretical codes adoption echo application, not emergence, and hence the posture that "the theoretical questions that researchers pose arise from the particular issues grounded in the studied empirical world" (Charmaz, 2008, p. 161).

3.4.4. Rationale for adopting ConGTM

In as much as it applies to all grounded theorists, the premise that the researcher can refer back to the setting to ask the interviewees further, supplementary precise questions to clarify the developing theoretical categories is an attractive benefit. The flexibility of grounded theory strategies is interesting as the researcher may adapt them to suit the exigency of the enquiry (Charmaz, 2008). Importantly, the researcher has flexibility to choose and create the methods as the research progresses. Constructivist grounded theory offers transparent analytic guidelines that afford researchers to make transparent analytic choices and constructions. During the research process, the researcher can create and see a straight connection linking data and conceptual categories. The researcher is not the observer in the research data analysis, but an active participant. Constructivist grounded theory is in line with contemporary thinking which the research subscribes to. The positivistic principle of a neutral observer, as advocated by Glaser and Strauss, emerged as problematic to the beliefs of the researcher which are aligned to social constructivist ontology. Constructivist grounded theory considers broader environmental and contextual factors that influence the phenomenon under study. It also aims to produce a theory that is relevant (theory that fits the situation) to guide the action in practice. It is recognised that the broad goal of all grounded theory approaches is to generate theory. The data analysis guidelines are considered helpful.

3.5. STUDY POPULATION

Cooper and Schindler (2001, p. 69) stated that "a population is the total collection of elements or participants about which the researcher makes some inferences". A population is necessary to draw a sample from (Cooper & Schindler, 2001). For this enquiry, the target population consisted of IT professionals encompassing IT auditors, IT risk management specialists/practitioners, and PCS professionals such as telecommunications network engineers and other professionals working on, and supporting municipal information infrastructures. The rationale for the population selection is based on the perceived roles they have in cyber-security towards safeguarding the information infrastructures.

Research participants selected for interviewing must be expert participants possessing prior experience with the phenomenon to be able to offer the researcher useful information. The ConGTM adopted in the enquiry endorses open-ended interview, conversational, and is mutually constructed, thus ensuring the required depth, richness and rigour. The ConGTM recommends fewer participants compared to descriptive statistical research methods. The number of participants in this qualitative research was 33.

3.6. DATA COLLECTION

This enquiry adopted semi-structured interviews as a method for data collection which is in line with ConGTM. During the study duration, collection of data and data analysis occurred simultaneously, as is the norm for GTM. Also as a tenet of grounded theory, purposive sampling was adopted to select the participants. The selection of research participants was based on their roles and responsibilities in the municipality's information infrastructures. The study site for the ConGTM enquiry was eThekwini Metropolitan Municipality in KwaZulu Natal Province of South Africa. The choice was prompted by the fact that the researcher is a citizen of this municipality and it was thus not expensive to collect data since limited travel was involved.

The ConGTM is focused on finding emergent concepts from a few, but intensive, data collection processes compared to seeking generalisation and representation as is the gist of other research approaches.

The researcher was able to ask for more detail during the interview process as he could probe back and forth into an issue being discussed as important points emerged, and could request for more clarification (Charmaz, 2006). Potential participants were systematically gathered through their roles in cyber-security in relation to the municipal information infrastructure. The data collection process was iterative and evolutionary and hence the total number of potential participants was not predetermined. The participants represented a diverse mix of personalities, each having different experiences, authority and expertise in the domain of IT and PCS (including management). The participants were all viewed as specialists in their various fields of work. One-on-one semi-structured interviews that lasted between 30 and 60 minutes were conducted, and each was conducted at the various participants' work place. Five pre-prepared questions were asked during the semi-structured interviews.

As outlined by Patton (1990, p. 317), the guidelines for conducting an effective interview were adopted. The guidelines adopted included attentively listening and appropriately responding to indicate to the participant that they were being heard (Patton, 1990). During the interview process, the researcher participated in the content of what the respondents were alluding to as both the researcher and participants were active participants in data collection. The researcher applied understandable and proper language, to communicate clearly, and to let the participant know how the interview was progressing, built rapport with the participant, and showed respect for the participant as a person.

3.7. THEORETICAL SAMPLING

Sarantakos (2005, p. 166) argued that theoretical sampling is based on choosing consequent interviewees based on the emergent information from the already coded data. The intention is to choose participants which will provide data that is relevant to the research (Sarantakos, 2005). Theoretical sampling is a technique of data sampling for the development of a theoretical category and is conducted only after a researcher has tentative categories to develop or refine (Charmaz, 2008). Emergent categories form the basis of theoretical sampling and, as a result, the researcher cannot anticipate where theoretical inquiry will take them. Through the analytic process, tentative categories arise and thus lead to new research sites and substantive areas. The enquiry conducted theoretical sampling until theoretical saturation was reached. Theoretical saturation happens when collecting more data yields no further views on the properties of the theoretical category.

3.8. DATA ANALYSIS

In the GTM, data analysis is a continuous process of analysing data through methodical filtering and the arranging of data obtained from interviews and any other data collection process. Data was reduced through manageable units for coding. Data analysis took place in parallel with data collection, and this was in accordance with GTM. Data was analysed until saturation was reached, meaning until no new information or additional information could be obtained from the collected data. Collecting, simplifying, transforming data into categories is another form of data analysis (Miles & Huberman, 1994).

3.8.1. Coding data

In GT, coding begins the emergent process of analysing data and is made up of at least two stages which are initial coding and focused coding (Charmaz, 2008). Initial coding enables the researcher to concentrate on the probable logic of the data while interrogating it. The researcher was cognisant of the fact that emergent leads could be gained through identifying in vivo codes (these are research participants' direct statements) which aid the researcher in understanding participants' meaning and in elucidating emergent actions (Charmaz, 2008).

Focused coding followed after the open coding. The researcher focused on the initial codes that were most frequent from the data collection. The researcher sorted and synthesised large amounts of data, scrutinised the codes more in order to assess the ones that described best or interpreted the empirical phenomenon (Charmaz, 2008). Tentative theoretical categories were derived from focused codes. By applying an analytical approach, the researcher linked the theoretical categories to develop the conceptual theory.

3.8.2. Memo writing

Ideas in process and in progress during the enquiry were captured through memo writing. Memoing (memo writing) is also a tenet of GTM. According to Charmaz (2008), memos can be partial, tentative, and exploratory. Through memo writing, the researcher gets the opportunity to discover more about the data. In terms of the memo guidelines provided by Charmaz (2008, p. 166), the following was done:

> *title the memos for easy sorting and storage; (2) wrote memos throughout the entire research process; (3) defined the code/category by its properties found in the data; (4) delineated the conditions under which the code/category emerged, maintained, and changed; (5) compared the code/category with other codes and categories; (6) included the data from which the code or category was derived right in the memo; (7) outlined the consequences of the code/category; (8) noted gaps in the data and conjectures about it.*

3.8.3. Theoretical saturation

Theoretical sampling and theoretical saturation are two key processes of CGTM. Theoretical sampling was guided by the theoretical saturation. Theoretical saturation is whereby the researcher reaches a point where no additional information or new concepts are emerging from the new data that is collected. Thus, repeated occurrences of similar data could be an indication that a point of saturation has been reached and data collection can then stop. Theoretical saturation is a situation whereby all the research concerns are clear and the theoretical framework does not change or improve at all. Thus, at this point further data collection will be simply confirming the theoretical proposition already developed and known rather than modifying or further explaining it.

3.9. CREDIBILITY, ORIGINALITY, RESONANCE AND USEFULNESS

The research was guided by Charmaz's (2006) four criteria for credibility, originality, resonance, and usefulness. The four criteria aided the researcher to address the implicit actions and meanings in the phenomenon investigated and helped to analyse how it was constructed (Charmaz, 2006). The researcher sought to answer the four criteria associated questions in the affirmative way in order to comply with the GT guidelines.

Table 3.3: Criteria for improving GT

Criteria One - Credibility
1. “Has your research achieved intimate familiarity with the setting or topic? 2. Are the data sufficient to merit your claims? Consider the range, number, and depth of observations contained in the data. 3. Have you made systematic comparisons between observations and between categories? 4. Do the categories cover a wide range of empirical observations? 5. Are there strong logical links between the gathered data and your argument and analysis? 6. Has your research provided enough evidence for your claims to allow the reader to form an independent assessment - and agree with your claims?”
Criteria Two – Originality
1. “Are your categories fresh? Do they offer new insights? 2. Does your analysis provide a new conceptual rendering of the data? 3. What is the social and theoretical significance of this work? 4. How does your grounded theory challenge, extend, or refine current ideas, concepts, and practices?”
Criteria Three – Resonance
1. “Do the categories portray the fullness of the studied experience? 2. Have you revealed both liminal and unstable taken-for-granted meanings? 3. Have you drawn links between larger ‘collectivities’ or institutions and individual lives, when the data so indicate? 4. Does your grounded theory make sense to your Interviewees or people who share their circumstances? Does your analysis offer them deeper insights about their lives and worlds?”
Criteria Four – Usefulness
1. “Does your analysis offer interpretations that people can use in their everyday worlds? 2. Do your analytic categories suggest any generic processes? 3. If so, have you examined these generic processes for tacit implications? 4. Can the analysis spark further research in other substantive areas? 5. How does your work contribute to knowledge? How does it contribute to making a better world?”

Source: Charmaz, K. (2006). Constructing grounded theory. A practical guide through qualitative analysis (p. 182-183). London: SAGE Publications.

3.10. GROUNDED THEORY GUIDELINES FOR IS STUDIES

A refined set of GT guidelines was established by Urquhart *et al.* (2010) for researchers within the IS discipline. Throughout the enquiry the researcher was guided by these guidelines for theoretical analysis.

Table 3.4: GT guidelines for IS studies

1. Constant comparison	This advice encourages both rigorousness and theory formulation. It involves repetitively associating instances of data labelled as a particular class with other instances of data in the same classification. Theory development is supported by uncovering the analytic properties of the codes and categories to rigorous analysis.
2. Iterative conceptualization	This recommendation recommends the intensification of the amount of abstraction and link categories through iterative conceptualisation. It is achieved through the process of theoretical coding which assist to understand the relationships amongst concepts or theory factors. Memoing is another important process in theory coding development and the iterative conceptualisation process.
3. Theoretical sampling	This guide emphasises the necessity of selecting research sample that is based on analytic grounds. It promotes theory development that is truly grounded in the data thereby ensuring the comprehensiveness nature of the emergent theory.
4. Scaling up	This recommendation advocates solution to what is thought to be a common grounded theory problem, viz. the generation of low level theory which is difficult to relate to the broader literature. It involves grouping higher-level categories into broader themes thereby contributing to theory generalisability.
5. Theoretical integration	This recommendation assist the researcher to relate the emergent theory to other theories in the similar field. It is important to compare the formulated substantive theory with other existing theories and this could help in formal theories generalisation.

Source: Urquhart, C., Lehmann, H., & Myers, M. D. (2010). Putting the 'theory' back into grounded theory: Guidelines for grounded theory studies in information systems. *Information Systems Journal,* vol. 20, no. 4, p. 369.

3.11. CHAPTER SUMMARY

The chapter discussed the design and approach that was followed to execute this research. The researcher's chosen paradigm was presented, GT was the chosen methodology and specifically the ConGTM. Three GTMs were discussed, namely Constructivist, Straussian, and Glaserian. Further, the rationale for adopting the ConGTM was provided. The research population, data collection process, and data analysis procedures were all deliberated upon. Lastly, the GT guidelines for achieving credibility were discussed.

CHAPTER 4
EMPIRICAL STUDY

4.1. CHAPTER INTRODUCTION

This chapter discusses the empirical enquiry of which the aim was to examine cyber-security capacity in metropolitan municipalities in South Africa. The sections covered in this chapter are discussed in Table 4.1.

Table 4.1: Structure of Chapter 4

	Topic	**Overview**
4.1	Chapter introduction	Presents an outline of the chapter.
4.2	The study site	Background on the site where enquiry was conducted.
4.3	Research participants	Discusses the research participants.
4.4	Research design and data collection	Presents the steps followed to conduct the enquiry.
4.5	Chapter summary	Presents highlights on topic covered in the chapter.

The researcher identified the general research problem, which was to investigate how cyber-security capacity in South African metropolitan municipalities could be assessed. Assessing cyber-security capacity entailed determining the structures, processes and relational mechanisms that the municipalities have implemented to manage cyber-security business risk facing the organisation.

4.2. THE STUDY SITE

The empirical study was conducted in the only metropolitan municipality found in the Province of KwaZulu-Natal (KZN) in South Africa. EThekwini Municipality covers an area of roughly 2555km2 and was home in 2016 to some 3.7 million people (ETh-IDP, 2017). As enshrined in *Section 155 (1) of the South African Constitution of 1996*, the Municipality is Category A, which means it has exclusive municipal executive and legislative authority in its area. The population in the municipality represents 33, 7% of the provincial population and 6, 6% of South Africa’s total population (ETh-IDP, 2017).

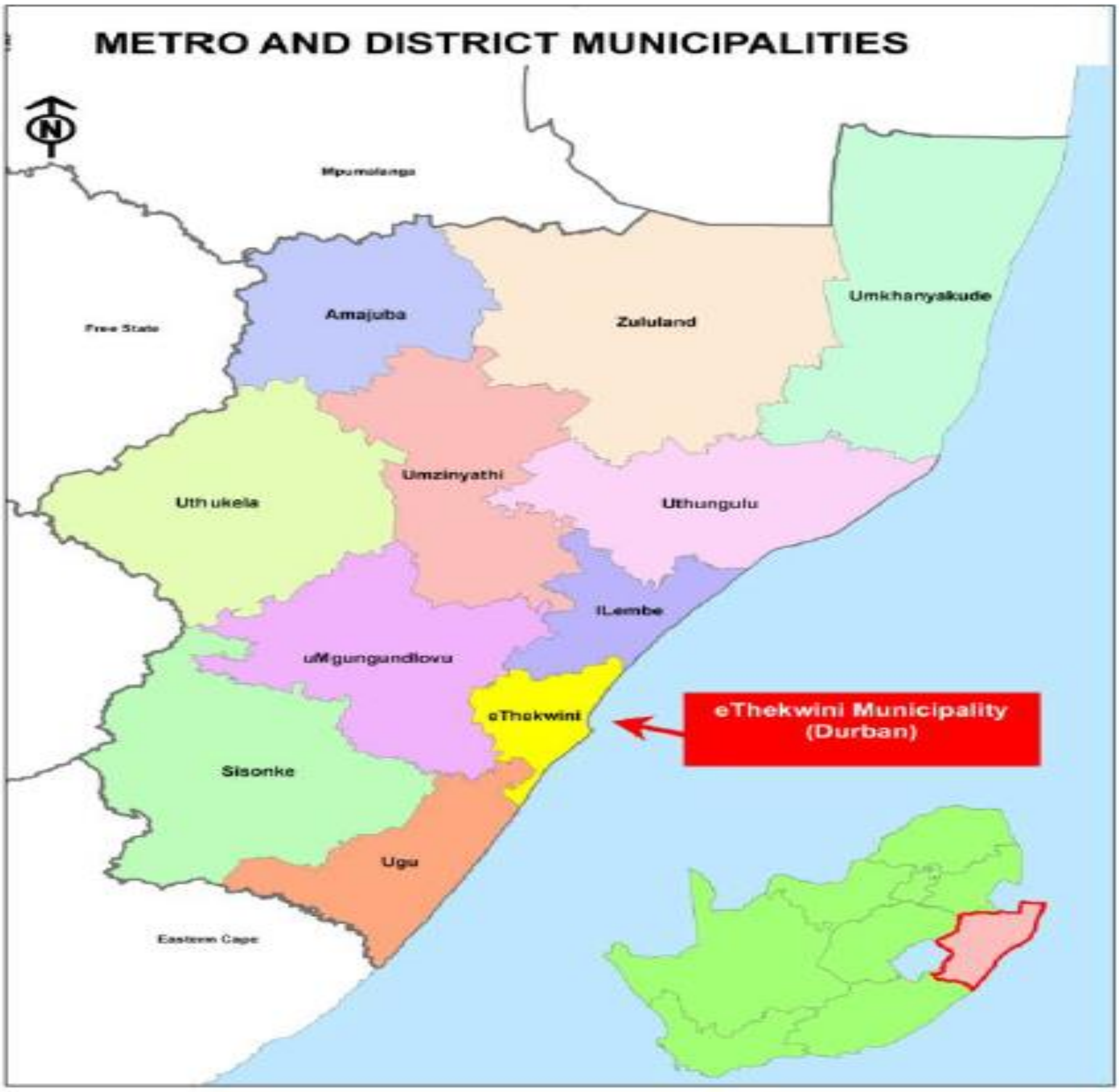


Figure 4.1: Districts and metropolitan municipalities in KZN

Source: EThekwini Municipality Integrated Development Plan (ETh-IDP). (2017). Durban: EThekwini Municipality, p. 32.

The economic powerhouse of KZN, the eThekwini Municipality, makes a significant contribution to the South African economy and is an important link between the regional economies of Pietermaritzburg and Richards Bay. The municipality offers 10% of all employment opportunities in the country (ETh-IDP, 2017). Ranked as the second largest economic centre, the municipality is the second most significant industrial region in the country and is a promising global competitor with a world-class manufacturing sector (ETh-IDP, 2017). Being home to Africa’s first multimodal logistics platform, eThekwini Municipality has an international passenger airport and that is King Shaka International Airport. The municipality is home to Africa’s busiest port which is Durban Port; and has an international conferencing centre, which is the Durban International Conference Centre. It is also regarded as South Africa's playground and tourist destination. The municipality provides essential public services within its jurisdiction. Being a coastal municipality with a large manufacturing base, eThekwini Municipality like any other government institution in the country, is at risk and vulnerable to a range of technological, natural, man-made and environmental disasters.

The Rockefeller Foundation launched the *100 Resilient Cities Centennial Challenge* (100RCCC) to enable cities globally to better address the 21st century major challenges, and to assist in the building of urban resilience. Urban resilience is the ability of the city to withstand continual stress and acute shocks while at the same time sustaining the provision of essential functions. 100RCCC prepares cities to cope with future changes. As a pioneer for the *100 Resilient Cities Centennial Challenge*, the City of Durban was selected as one of 372 cities internationally to apply for the 100RCCC. In December 2013, it was selected as one of the first cohort of 33 successful cities to be inaugurated into the 100 Resilient Cities (100RC) Programme (ETh-IDP, 2017). The City of Durban has to face up to the challenge of translating global ideas around resilience into our local context. The eThekwini Municipality as local sphere of government is particularly susceptible to changes to environmental, social, and economic systems, with many citizens vulnerable to lack of adequate housing, access to sanitation and waste removal, safe drinking water, a healthy natural environment and adequate health care facilities. To avoid exacerbating an already fragile situation, it becomes important how the municipality plans and prepares for these challenges such that it can respond effectively to current and future changes. The opportunity to participate in the 100RC Programme provides the municipality with the prospect of starting to consider and plan in a coordinated and innovative way on resilience issues and to stimulate the needed support to implement action around key resilience priorities for the city.

This study sought to enhance the implementation of cyber-security at local government level. At a national government level, in 2015, the country published the NCPF which stresses the importance of cyber-security implementation at local government level. *The Constitution of the Republic of South Africa* (RSA, 1996) requires local government to ensure the provision of services to communities in a sustainable manner, promote social and economic development, and promote a safe and healthy environment. *Section 41(1)(b)* further requires all spheres of government to secure the well-being of the people of South Africa. Some municipal essential services are effectively and efficiently provided to communities through the utilisation of cyberspace. Participating in cyberspace presents colossal challenges to the municipality and hence for institutional arrangements to manage the information, critical infrastructures need to be better structured. The country's *National Development Plan (NDP) vision 2030* put forward the need of establishing a municipal fibre-optic network to provide the backbone for broadband access to meet social objectives.

Municipalities in South Africa are required by the Municipal Systems Act (No.32) of 2000 (RSA, 2000) to prepare Integrated Development Plans (IDPs) which comprise a key component in entrenching government principles. Municipalities deliver the community needs through IDPs. EThekwini Municipality has aligned the IDP with international, national, provincial, and local developmental policies (ETh-IDP, 2017). The services provided by the municipality to the eThekwini citizens include clean water, energy, and emergency services. The municipality uses an information infrastructure to support the administration of the city.

4.3. RESEARCH PARTICIPANTS

The research participants were employees of eThekwini Municipality. The municipality has diverse departments. To achieve the research intentions, the study participants were purposively selected based on their role to implement cyber-security initiatives to safeguard the information infrastructure from cyber-security vulnerabilities. The participants were selected from different departments which are ICT, Water and Sanitation, Electricity, and Finance. Thirty-three participants were intensively interviewed with the aim of achieving the research objectives. The rationale on the total number of research participants was based on the theoretical sampling and theoretical saturation. The composition of the participants comprised employees working in both streams of ICT, and PCS. The participants working on ICT were selected on the basis that ICT forms part of information infrastructure. PCS participants were chosen on the basis that PCS, such as SCADA, are largely dependent on ICT. The industrial control systems form part of the information infrastructure in the municipality. Industrial processes are remotely controlled through the use of a SCADA tool, the functionality of which is embedded in the ICT infrastructure. The professions of the participants varied and comprised a range of different skills.

Table 4.2: Profile of research participants

Based on theoretical sampling and theoretical saturation			
Stream	**Department**	**Profession**	**Number**
ICT	ICT	ICT Networks	3
		Software Development	3
		Systems Support	3
		User Support	4
Assurance & Risk Management	IT Audit	IT Audit Specialists	2
	IT Risk Management	IT Risk Specialists	2
PCS	Water and Sanitation	Computer Network Systems	4
		Water SCADA	4
	Electricity	Computer Network System	4
		Electricity SCADA	4
Total			33

4.4. RESEARCH DESIGN AND DATA COLLECTION

The road map of the enquiry design adopted is outlined in Figure 4.2.

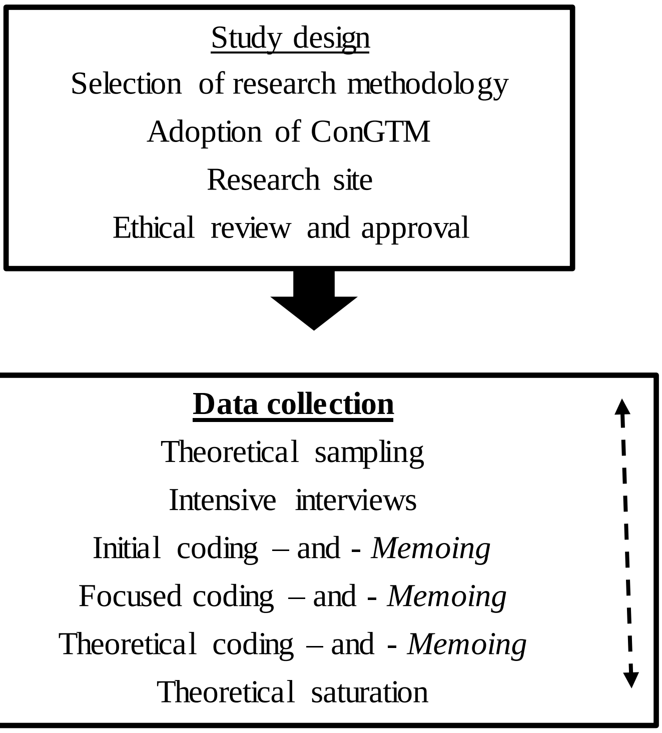

Study design
Selection of research methodology
Adoption of ConGTM
Research site
Ethical review and approval
Data collection
Theoretical sampling
Intensive interviews
Initial coding – and - *Memoing*
Focused coding – and - *Memoing*
Theoretical coding – and - *Memoing*
Theoretical saturation

Figure 4.2: Research design and data collection

4.4.1. Ethical review and approval

The research complied with the UKZN's ethical processes. The application for ethical clearance was submitted to the Humanities and Social Sciences Research Ethics Committee, and was approved. The application included a completed "Ethical Clearance Application form", copy of the gatekeeper's letter that was signed by the eThekwini Municipal Manager, participants' information sheets, consent forms, and initial interview protocol and questions. The ethical clearance reference number was HSS/0894/017D.

4.4.2. Data collection

The researcher prepared five semi-structured interview questions as an instrument to collect data. Intensive interviewing permitted an in-depth exploration of cyber-security status through the participants' experiences in implementing cyber-security to safeguard municipal information infrastructures. In alignment with GTM, the first group of research participants encompassing both ICT and PCS professionals was interviewed following theoretical sampling. The second group of participants which also encompassed both streams, and various professions, was interviewed to confirm the initial codes that had been developed from the first group of interviews. The final set of interviews was conducted to achieve theoretical saturation.

4.4.2.1. The interview questions

Excluding the questions related to biographical information, three semi-structured interview questions were prepared by the researcher. The research questions aimed at answering the study's core research question. The main objective of the research was to determine the cyber-security status in the metropolitan municipalities in South Africa. The concepts of cyber-security and information infrastructure were discussed with the each participant before the start of the interviews. The participants were asked the interview questions as presented in Table 4.3.

Table 4.3: Semi-structured interview questions

	Question	Objective
1.	How is eThekwini Metropolitan Municipality protecting organisational information infrastructure assets against cyber-threats?	The objective of the question was to explore the practices that eThekwini Metropolitan Municipality has implemented to protect organisational information infrastructure assets against cyber-threats.

2.	What methodologies are currently available to assess the cyber-security status in the eThekwini Metropolitan Municipality?	The objective of the question was to explore the methodologies currently employed to assess the cyber-security in the eThekwini Metropolitan Municipality.
3.	How is eThekwini Metropolitan Municipality inculcating the culture of cyber-security across the organisation?	The objective of the question was to understand the processes that are employed to provide an enabling environment to develop, implement, and sustain a cyber-security culture in organisation.

The duration of each interview conducted was between 45 and 60 minutes. The researcher captured the proceedings of the interviews on his laptop during the interview session. The interviews details were transcribed in compliance with confidential consideration of the ethical clearance. Interviews were conducted until no new information could be obtained from participants in relation to achieving the research objectives.

4.4.3. The two coding processes

The two coding phases were undertaken, namely initial coding and focused coding. Data analysis was iterative and was conducted at the same time as data collection. The coding process applied in the study was adopted from ConGTM of Charmaz (2006) and is presented in Figure 4.3.

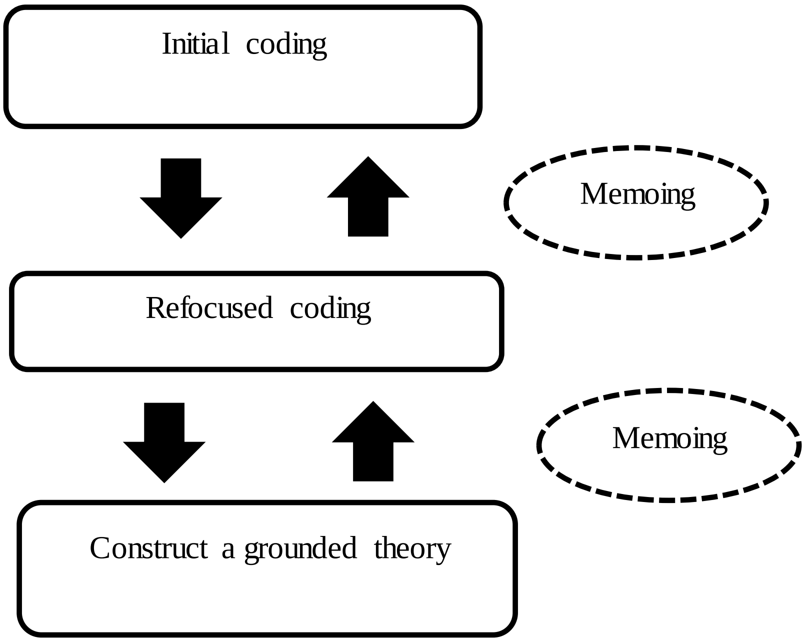


Figure 4.3: Coding process adopted

4.4.3.1. Initial coding

This was the first phase of coding undertaken after each of the data collection and interview transcriptions. The research worked closely with the data and tried to understand each sentence in terms of identifying what exactly was meant by the respondent. Initial codes were formulated and treated as provisional because the researcher wanted to remain open to other analytic possibilities and create codes that best fit the data at hand. The research concentrated on the codes that indicated that they fit the data and the phenomenon being studied. Concurrent data analysis and data collection assisted the researcher to go further and deeper into the research problem. During the analysis, the researcher kept codes active, analytic, short, and simple. An attempt was made to code with words that reflected action. As the first step, line-by-line coding was employed, meaning naming each line of written data. However, not every line contained a complete sentence and not every sentence could appear to be important. During line-by-line coding, the researcher could identify implicit concerns as well as explicit statements, and this assisted to refocus later interviews.

Table 4.4: List of initial codes for Question 1

1. Municipality develops, and implements the IDP	2. Comply to applicable legislation and regulations	3. Authority originates from the Constitution of RSA
4. Provide essential services to the public	5. Municipal council is the highest decision-making body	6. Day-to-day highest decision making is delegated to Exco
7. Exco comprises of politicians	8. Municipal manager reports to Exco	9. Municipal manager leads the municipal administration processes
10. Municipality comprises of various functional domains	11. Functional domains are made of various business units	12. Business units are led by unit heads
13. Unit heads implement municipal vision	14. Unit heads implement municipal strategies	15. Unit heads implement municipal policies
16. Management of finances is guided by MFMA	17. Corporate governance is guided by the King IV report	18. Exco delegates policy development to the municipal manager
19. Municipal Systems Act guides the implementation of performance management systems	20. Senior management comprise municipal managers, and deputy municipal managers,	21. Municipal manager leads the senior management team
22. Municipality provides services to the public	23. Various business units provide essential services	24. Water and sanitation is an essential service provided
25. Provision of electricity is an essential service provided	26. Various forms of infrastructure are further services provided	27. Municipal administration requires ICT support
28. Efficient provision of essential services requires process automation	29. Process automation is entrenched in ICT	30. Process automation is made up of PCS
31. Water SCADA system is an example of PCS	32. Electricity SCADA system is an example of PCS	33. MFMA guides the establishment of the internal audit function
34. Governance processes are executed by senior management team	35. Various committees have been developed to provide oversight on municipal processes	36. Infrastructures committee provides oversight on municipal infrastructure assets

37. Finance committee provides oversight on municipal finances	38. Audit committee provides oversight on the internal controls that management has implemented to mitigate the identified risks	39. Audit committee provides oversight on the governance processes that management has implemented
40. Audit committee provides oversight on the internal risk management processes that management has implemented	41. Senior management team has developed cyber-security steering committee	42. Composition of cyber-security steering committee is made up of senior management officials responsible for delivery of essential services
43. Cyber-security steering committee is guided by the cyber-security steering committee charter	44. Cyber-security steering committee charter should be reviewed annually	45. Cyber-security steering committee should develop cyber-security policy
46. Cyber-security steering committee advise Exco on cyber-security matters	47. Cyber-security steering committee approves cyber-security implementation plan	48. Cyber-security steering committee approves cyber-security annual operational plan
49. Audit committee approves the three-year risk-based rolling plan	50. Audit committee approves the internal audit annual operational plan	51. Internal audit function provides assurance on the municipal performance information
52. Formulate central point for addressing and coordinating cyber-security municipal-wide	53. Cyber-security policy to extend from information security policy	54. Cyber-security policy encompasses all information infrastructures beyond IT unit
55. Internal audit function provides assurance on the implementation of IT governance processes	56. Senior management has implemented risk management processes across the organisation	57. Senior management has developed a portfolio responsible for strategic assets management
58. Senior management has developed supply chain management policy	59. Senior management has developed skills development policy	60. Senior management has developed recruitment policy

61. Unit heads are responsible for the functional/operations effectiveness of their business units	62. Unit head provides methodologies to safeguard organisational assets guided by pertinent policies, legislation, and regulations	63. Unit heads develop and implement business continuity strategies
64. Unit heads develop and implement disaster recovery strategies	65. Various units adopt industry best practices to achieve consistent results on their business objectives	66. Supply chain management processes include vendor/supplier management practices
67. ICT unit is responsible for protecting information assets in the municipality	68. Business units develop and continuously maintain the risk registers	69. Senior management team develops and continuously maintains strategic risk register
70. Unit heads develop and maintain their respective operational risk registers	71. ICT unit plans/designs corporate/organisational telecommunication networks	72. Business units who own PCS plan/design their specific computer networks
73. ICT unit implements hardware and related software to run and protect the corporate telecommunication networks	74. ICT unit implements hardware and related software to monitor corporate computer network activities	75. ICT unit is responsible to implement information security policy
76. ICT unit conducts continuous computer network vulnerability assessments	77. Various business units conduct contingency plans testing	78. ICT unit deploy technologies to monitor, detect, prevent unauthorised access to organisational computer networks
79. The basis of business processes is to deliver services to the local citizens	80. IDP is the service delivery framework in the municipality	81. Expenditure is linked to the IDP which is reviewed annually
82. Information infrastructures support business processes in pursuit of service delivery	83. Critical infrastructures are supported by information infrastructures	84. Each business unit manages its own cyber-security affairs.

85. Business units that own PCS deploy technologies to monitor, detect, prevent unauthorised access to their computer networks	86. ICT unit has developed and implemented IT assets maintenance plans	87. Business units that own PCS have developed and implemented their infrastructure maintenance plans
88. Through IT governance processes, ICT has adopted industry best practices such as Cobit	89. ICT unit participates in IT systems acquisition processes	90. Human resources unit implements the recruitment policy
91. Before joining the employ of the municipality, employees are vetted in terms of qualifications, and previous work experience	92. Various business units develop and submit for approval their annual budgetary requirements	93. Various business units conduct skills development for their employees
94. Various business units conduct continuous professional development	95. Various business units conduct cyber-security user awareness and training in cyber-security	96. Various business units encourage staff to get certified on their various occupations
97. Various business units encourage staff to join and participate in their professional institutes	98. On employee on-boarding, HR conduct induction and it includes cyber-security, and the obligation of each employee to maintain and enhance cyber-security within the organisation	99. On employees exiting the employ of the municipality, HR communicates the termination details to ICT unit to terminate access to IT assets
100. Audit on IT system is conducted by internal audit unit	101. Control weakness identified during the audit process is communicated with senior management for subsequent rectification of those controls	102. Internal audit reports are communicated to the audit committee to maximise accountability

103. Various business units have implemented physical protection on their infrastructures	104. Various business units have implemented access controls into their information infrastructures	105. Service level agreements as part of the SCM processes have been implemented
106. Punitive clauses are incorporated in the service level agreements in case of poor delivery and non-compliance	107. ICT unit communicates the computer network statistics to various business unit heads	108. Breach of security is communicated to the process and information infrastructure owner
109. Access to information infrastructure is restricted to only authorised employees, consultants, and service providers	110. Computer networks intrusion detection tools are implemented and monitored continuously	111. Ant-virus software is implemented and maintained
112. ICT unit has developed the information security portfolio	113. Software development process embed information security principles	114. IT acquisition includes security testing process
115. Internet usage is monitored	116. ICT has implemented web security processes	117. Access control processes include authentication mechanism
118. Sensitive data communicated over computer networks is encrypted	119. ICT unit conducts systems back-up procedures	120. ICT unit has developed and implemented cyber incident management procedures
121. System logs are generated and checked by responsible officials	122. Systems administrators' privileges and access rights are monitored	123. ICT unit has implemented IT service desk
124. Units that have implemented PCS have established 24/7 computer networks monitoring centres	125. Disaster recovery plans for information infrastructures are continuously tested	126. Business units encourage their staff to attend seminars and breakfast sessions normally hosted by professional institutes
127. ICT educate end-user on cyber-attacks	128. Where network vulnerability testing has been conducted,	129. ICT unit has implemented IT assets disposal policy

including social engineering	penetration testing is conducted	
130. Remote access to organisational information infrastructure assets is controlled	131. Operating systems default passwords are controlled	132. Collaboration on cyber-security amongst various departments takes place
133. Various business units participate in research and development activities	134. Tertiary education institutions partner with various business unit on cyber-security related matters	135. Each employees' performance assessment is conducted on a quarterly basis
136. ICT and the data therein are the underlying causes for cyber vulnerability	137. Adoption of ICT is the underlying cause of cyber vulnerability	138. ICT is the core of information infrastructure
139. Municipality implemented disciplinary processes for non-compliance and breach of security by employees	140. Downloading software is restricted to authorised individuals	141. Uploading of software to the organisational information infrastructure is restricted to authorised employees
142. Suspected mischievous actions on information infrastructures are reported to forensic investigation unit and subsequently to SAPS	143. ICT unit communicates information security policies across the organisation	144. Changes to information infrastructures are tested before effected
145. Software development methodology is prescribed for system testing before implemented to live environment	146. ICT unit provides guidelines on the complexity of IT system users' passwords	147. Users are made time-out if there is inactivity for a specified amount of time in a session
148. Log-in attempts are monitored and reported to relevant management	149. A cap has been set on unsuccessful log-in attempts in computer networks and IT systems	150. Various business units have implemented segregation of duties control
151. Various business units are conducting	152. External independent assessments are	153. Investment on cyber-security

health checks on the information infrastructures	conducted on the security of information infrastructure assets	projects/implementations is monitored and reported on
154. Trustworthiness of employees working on information infrastructures is a serious consideration	155. Employees' ethical behaviour is one of the factors to consider when addressing protection of information infrastructure	156. Commitment by employees to protect information infrastructures is essential
157. Individually, employees sign the e-mail use policy	158. Individually, employees sign the Internet use policy	159. Various business units are monitoring compliance with the acceptable use of information infrastructures
160. Systems documentations including user manuals are developed and maintained	161. Individual employees are encouraged to attend relevant professional conferences in order to understand current trends on cyber-security	162. Municipality has formulated a technical working group on cyber-security, whose composition includes both streams of ICT and PCS
163. Legal unit has identified relevant legislation and regulation pertaining to information infrastructures	164. Independent consultants are engaged to test compliance to pertinent IT laws and regulations	165. Governance audits are conducted to assess the effectiveness of governance structures and processes
166. Management provides budget and prioritises skills development for employees working on information infrastructures	167. Office of the Auditor General conducts audits on information infrastructures	168. ICT unit has implemented network perimeter control on corporate networks

Table 4.5: List of initial codes for Question 2

1. Various ICT audits are conducted annually by information infrastructures	2. Various ICT audits are conducted by the office of the Auditor General	3. State Security Agency conducts network vulnerability assessments or critical

		information infrastructures
4. Compliance audits on information infrastructures are conducted	5. Various business units conduct network monitoring, and subsequently generate statistics reports	6. Various business units conduct network vulnerability assessments
7. Various business units engage independent consultants to conduct various types of systems heath checks on information infrastructures	8. Independent assessors check the budget allocated to implement cyber-security processes	9. Independent assessors evaluate senior management involvement
10. Independent assessments are conducted to evaluate the effectiveness of various committees on cyber-security matters	11. Internal audit function assesses the design and effectiveness of governance processes that are related to cyber-security	12. Various business units on a continuous basis conduct controls of self-assessment on information infrastructure protection
13. External quality assessment reviews are conducted on internal audit function	14. Internal audit function conduct audits on risk management processes across the organisation	15. Internal audit reports to independent audit committee on cyber-security matters
16. ICT keeps records of computer networks down time	17. ICT unit keeps statistics on cyber-security user awareness training initiatives	18. Status on audit queries is kept by the internal audit function and other assurance providers
19. Number of employees with necessary qualifications and skills for protection of information infrastructure	20. Frequency of staff attending continuous professional development initiatives related to information infrastructure protection	21. Budget allocated to implement cyber-risk mitigation strategies
22. Presence of cyber-security risk in the strategic risk register	23. Presence of cyber-security risks in business units operational risk registers	24. Availability of the approved cyber-security policy
25. Availability of the cyber-security steering committee charter	26. Availability of cyber-security steering committee meetings	27. Availability of infrastructure committee minutes

28. Presence of cyber-security agenda item on infrastructure committee’s agenda	29. Frequency of cyber-security steering committee meetings	30. Number of cyber-attacks reported in the organisation
31. Number of devices infected by virus and related illicit software	32. Successful tests of DRP	33. Successful tests of BCP related to information infrastructures
34. Involvement of IT unit in information infrastructure acquisition processes	35. Testing of ICT system before implementation	36. Review and monitoring of ICT system logs
37. Individual performance assessment conducted	38. Signing of internet use policy by individual employees	39. Signing of e-mail use policy by individual employees
40. Internal business communication amongst various business units	41. Compliance to HR recruitment policies	42. Compliance to ICT related laws and regulations
43. Discussion of cyber-security in executive authority meetings	44. Assess the effectiveness of various oversight committees	45. Assess implementation of IT governance processes
46. Availability of tools to detect intrusion into organisational computer networks	47. Availability of tools to protect computer networks from unauthorised access	48. Availability of information infrastructure maintenance records
49. Availability of complete information infrastructure catalogue	50. Operating effectiveness of physical safeguarding of information infrastructure	51. Availability of functional access control to information infrastructure
52. Availability of tested cyber-security incident management procedures	53. Availability of network plans and designs	54. Adoption of industry best practices
55. Level of collaborations within and outside the organisation	56. Availability of statistics on log-in attempts	57. Number of staff engaging in research and development projects
58. Existence of collaborations and partnerships with tertiary institutions	59. Attendance to pertinent local and national conferences related to information infrastructure protection	60. Compliance to cyber-security policy assessment

61. Number of staff disciplined for breaching cyber-security policy	62. Working/implemented personal development plans on performance gaps identified during individual performance assessments	63. Compliance to pertinent municipal legislation and regulations
64. Controls implemented for remote access to organisational information infrastructure assets	65. Encryption of transmitted data	66. Availability of signed job descriptions for employees working on information infrastructure
67. Availability of Exco minutes where cyber-security was discussed	68. Deployment of network monitoring tools	69. Deployment of network security tools
70. Availability of information infrastructure disposal procedures	71. Communication on various cyber-security-related policies	72. Adoption of international standards
73. Conducting social engineering tests	74. Time it takes to solve audit queries raised on cyber-security weakness	75. Availability of cyber-security strategy
76. Adoption of industry best practices on risk management processes	77. Adoption of industry best practices on ICT and PCS processes	78. Level of information between ICT and PCS domain
79. Reported/unreported unauthorised access to information infrastructure assets	80. Cyber-security-related incidents reported to forensic investigation unit and SAPS	81. Adoption of King IV report in corporate governance processes
82. ICT drive cyber-security implementation	83. Availability of information security portfolio within the organisation	84. Segregation of duties to individuals working on information infrastructure
85. Availability of information infrastructure asset management policy	86. Monitoring of systems administrators' activities in the computer system	87. Records of Exco training in cyber-security
88. Records of senior management workshops on cyber-security	89. Management monitoring of SCM policy-related information infrastructures	90. Availability of security reports on information infrastructures

91. Availability of records and documents related to information infrastructure changes implemented	92. Communication of changes to information infrastructures	93. 24/7 monitoring of cyber-security nerve centre for PCS
94. Availability of continuously tested backup procedures	95. Communication of cyber-security emergent risks/threats	96. Availability of bring your own device policy
97. Monitoring of VPN	98. Information workshops conducted on cyber-security across the organisation	99. Continuous security clearance procedures on employees working on information infrastructures

Table 4.6: List of initial codes for Question 3

1. Involve senior management in cyber-security processes	2. Involve Exco in cyber-security processes	3. Formalise cyber-security processes
4. Implement cyber-security policy	5. Develop, implement, and monitor implantation of cyber-security strategy	6. Monitor operational effectiveness of oversight committees
7. Sponsor cyber-security implementations	8. Continuously conduct risk assessment on cyber-security	9. Enforce compliance to cyber-security policy
10. Monitor compliance to cyber-security-related legislation and regulations	11. Conduct various types of ICT audits on information infrastructures	12. Comply with SCM policies related to information infrastructure
13. Implement performance management system	14. Implement and enforce compliance to industry best practices	15. Implement and enforce compliance to information security policy
16. Conduct continuous user awareness campaigns	17. Educate computer users on cyber-security risk	18. Comply with HR policies on recruitment

19. Assess individual employee performance assessments	20. Conduct research and development on cyber-security pertaining to information infrastructure	21. Monitor employee activities on the computer networks
22. Monitor compliance to MFMA	23. Monitor compliance to Systems Act	24. Monitor compliance to structures act
25. Promote individual continuous professional development	26. Maintain and sustain various collaborations that enhance information infrastructure protection	27. Subsidise employee formal education related to information infrastructure and cyber-security
28. Promote communication amongst various business units on matters related to cyber-security and information infrastructure	29. Conduct information security health checks across the organisation	30. Conduct assessments on governance processes' alignment to best practices such as King IV report
31. Implementation cyber-security enforcement tools	32. Remind users on good cyber-security practices	33. Users take accountability for cyber-security violations
34. Conduct risk assessments on information infrastructures	35. Conduct network vulnerability assessments	36. Automate security processes
37. Develop help desk to solve cyber-security-related problems across the organisation	38. Monitor remote access to information infrastructures	39. Align cyber-security to IDP processes
40. Manage cyber-security investments	41. Promote affiliations to occupational cyber-security related institutes	42. Conduct skills audit on employees working on information infrastructure
43. Allow staff to attend cyber-security workshops/seminars/breakfast sessions, etc.	44. Conduct continuous cyber-security assessment across the organisation	45. Conduct period test on social engineering
46. Make users understand the implications of non-	47. Make users/employees understand that	48. Continuously communicate to users to report

compliance to cyber-security polices	punitive mechanisms will be instituted on cyber-security policy violations	suspicious activities taking place on information infrastructure
49. Make users aware what to do if they experience cyber-attacks or mischievous activities in the organisational computer networks	50. Monitor internet usage, and make users aware that their activities on the Internet are monitored	51. Monitor e-mail system usage and make users aware that their usage of the e-mail system is monitored
52. Monitor current trends on cyber-security and communicate the emerging risk across the organisation	53. Cyber-security is driven from ICT unit	54. Investigate incidents of cyber-security breaches
55. Report statistics of cyber-security breaches to various business heads for consequence management purposes	56. Cyber-security implementation processes for efficiency and consistency purposes	57. Implement and monitor access control to information infrastructures
58. Conduct cyber-security health check inspections on information infrastructures	59. Promote collaborations between PCS and ICT streams	60. Implement and monitor cyber-security governance processes
61. Report progress on implementing cyber-risk mitigation strategies	62. Report continuously to cyber-security steering committee on the implementations of cyber-security operational plans	63. Test system security before implementations
64. Test changes to computer systems before implementations	65. Report cyber-security breaches to relevant portfolio committees	66. Enforce authentication to access information infrastructure
67. Conduct BCP test	68. Conduct DRP tests	69. Test back-up and recovery procedures
70. Keep records on information infrastructure maintenance	71. Centralise management of cyber-security implementations	72. Promote compliance to Occupation Health and Safety Act

4.4.3.1.1. Consolidated memoing for Question 1 initial coding

Charmaz (2006, p. 72) stated that "Memo-writing is the pivotal intermediate step between data collection and writing drafts of papers". During memo writing the researcher analysed ideas about the codes in any and every way possible, but related to the research objectives. Memoing kept the researcher entrenched in the analysis and helped to increase the level of abstraction of ideas. During memo writing, thoughts were recorded, comparisons were captured and connections were made for further considerations by the researcher. The researcher was an active participant and was thus an important instrument during the data collection and analysis phases. The processes of memo writing provided a space to become actively engaged in research, to develop ideas, and to fine-tune subsequent data gathering. Memo writing for formulation of Question 1 initial codes is presented in Table 4.7.

Table 4.7: Consolidated Memo writing for Question 1 initial codes

Consolidated memo writing for Question 1 after the initial codes
Question: How is eThekwini Metropolitan Municipality protecting organisational information infrastructure assets against cyber-threats?
Objective: The objective of the question was to explore the practices that eThekwini Metropolitan Municipality has implemented to protect organisational information infrastructure assets against cyber-threats.
Premise: "In grounded theory the analyst humbly allows the data to control him as much as humanly possible, by writing a theory for only what emerges through his skilled induction. The integration of his substantive theory as it emerges through coding and sorting is his verification that the hypotheses and concepts fit and work and are relevant enough to suggest. They are not proven; they are theory" (Glaser, 1992, p. 87).
Section 1 – Municipal mandate and authority to deliver services
A metropolitan municipality is a government service delivery machine. The Municipal Systems Act, No 32 of 2000 (RSA, 2000), requires all municipalities in the country to develop an Integrated Development Plan (IDP) to guide all developments in the municipality. IDP informs allocation of resources and municipal budgeting. IDP is a strategic development plan which spans for five years. IDP is owned by the municipal council, and is reviewed annually. IDP ensures that the municipality is accountable to the citizens and businesses located within the municipality. The development of the IDP is normally delegated to the municipal manager by the municipal council. For example, the eThekwini Municipality's IDP mentions global agendas which include the African Union agenda, New Urban agenda, the Paris agreement, and other commitments which the municipality is committed to achieve. In the 2017/18 eThekwini Municipality's IDP, the Mayor Councillor, Zandile Gumede, says "I am proud to say that as a City we have been actively involved in influencing policy and strategy at a Global, National, provincial and Local Government level" (Eth-IDP, p. 9).

Capacity to deliver services to the municipal public and businesses alike is important. Capacity ensures that the IDP is achieved as intended. Cyber-security is one amongst many capacities that the municipality needs to deliver services. Cyber-security spans across various sectors and business units within the municipality. A competent workforce is core to the delivery of effective and quality services in the municipality. To strengthen administrative governance, the municipality has integrated risk assurance in pursuit of effective and efficient service delivery. The adoption of IT assists the municipality to eliminate resources wastage, improve effectiveness, efficiencies and accountability. IT adoption also assists to develop a Smart City.

Some of the risks that are faced by the municipality include service providers' unavailability to provide much needed and essential services. Disruption to services raises the continuity risk exposure. Cyber-attack and unplanned information and telecommunication outages are some of the key risk drivers. Continuity risk if materialised results in the municipality being unable to deliver services to the municipality community. Cyber-security is essential to minimise or mitigate the risk of service delivery continuity.

The municipality has established an executive committee (Exco) which is the principal committee of the municipality. Members of Exco are politicians from political parties represented in Council in the same proportion. On a day-to-day basis, Exco is the highest decision-making body in the municipality on behalf of full Council (has delegated powers). There are portfolio committees (composition by councillors) that support Exco. These portfolio committees include the Human Settlements and Infrastructure Committee which "Considers and makes recommendations to the Executive Committee and Council on all matters pertaining to electricity, engineering, human settlements, transport, waste management and water & sanitation" (ETh-IDP, 2017, p. 485). There is also a Governance & Human Resources portfolio committee "responsible for corporate administration; national and international stakeholders; and human resources matters including skills development" (ETh-IDP, 2017, p.485).

There are also statutory committees which have been created in compliance with various Acts. Amongst these types of committees is the audit and risk committee whose comprise independent individuals who are not municipal employees or municipal councillors. The core of this committee is to advise Exco and senior management on the status of internal controls that management are implemented to ensure that municipal objectives are achieved, maintained, and enhanced. This committee also advises Exco on the risk management and governance process that the municipality has implemented in pursuit of organisational objectives and mandates.

Given the municipal strategic objectives, it has become apparent that ICT is a valuable municipal asset which enable municipal service delivery. Cyber-security is no longer an option for the municipality particularly taking into consideration that most essential services are entrenched in ICT. Participants have indicated that cyber-security is not only about technical solutions but also about human issues.

Section 2: Utilisation of process control systems in service delivery

Being a Category A Municipality, eThekwini Municipality offers a variety of services to the public under the jurisdiction of the municipality. The delivery of services is made possible in some functional areas through the utilisation of ICT. The interconnectedness of municipal computer networks makes it possible for the municipality to:

- distribute electricity to the municipality community
- distribute water to the Municipality community
- provide much needed administrative support across the municipality. ICT systems such as e-mails, Internet system, and enterprise resource planning systems, are examples of support systems in the municipality.

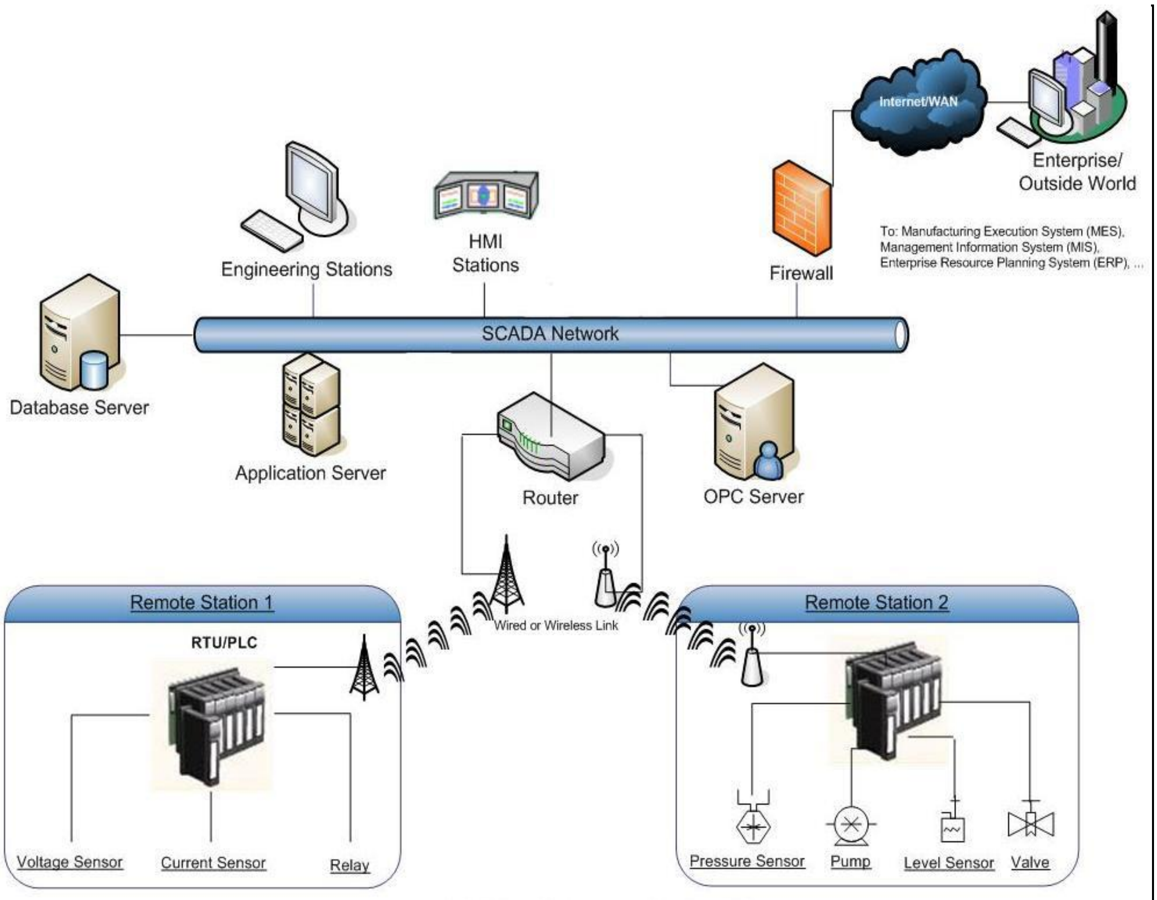
PCS for electricity

Electricity unit: through the use of SCADA system the unit delivers electricity to the citizens. SCADA is a form of a process control system (PCS). ICT is used to improve reliability, intelligent control, optimum operation, and protection of a power system network. The functioning of the PCS is entrenched on ICT. A SCADA system has advanced data collection capability, facilitates remote monitoring, and automates entire electricity distribution by coordinating, controlling and operating distribution components. As a PCS, SCADA enables the operator to monitor and control distributed systems at various remote geographical areas. SCADA is made up of computers, networks, controllers, instruments, actuators, and interfaces to manage automated industrial processes. SCADA systems are economical as they eliminate the visit of personnel to geographically dispersed locations to conduct inspections, make adjustments in the processes, and data collection.

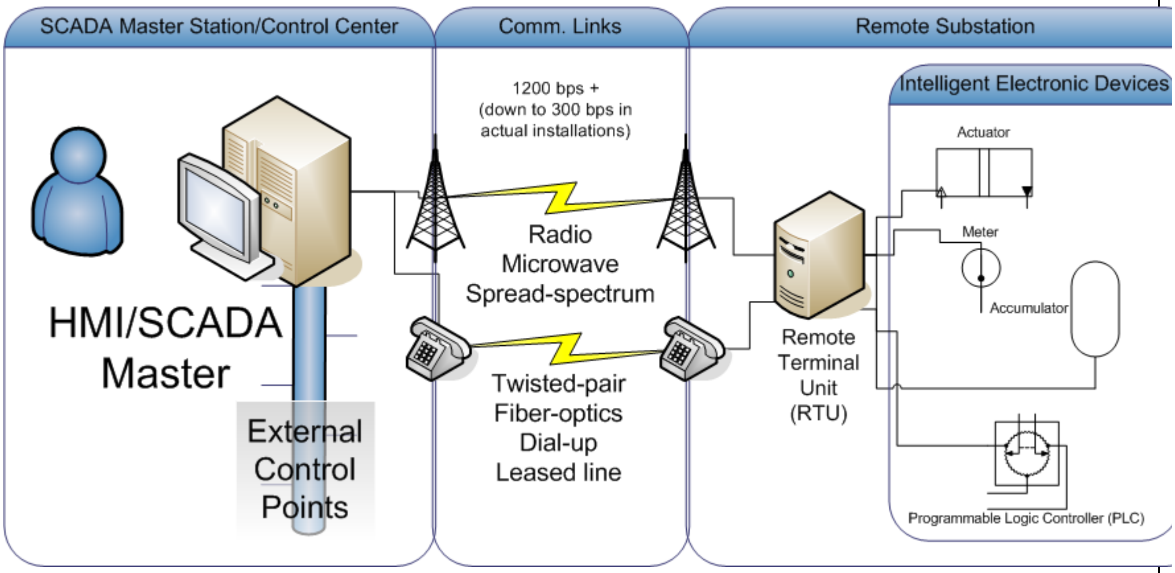
PCS for drinking water

SCADA systems measure, control, and monitor (locally and remotely): water collection and extraction, transport water to settling basins, transport water to filtration/purification processes, monitor and control filtration/purification processes, monitor treated water distribution, and monitor and control pressure boost pumps.

The following diagram shows the electricity distribution SCADA system



OpenControl SCADA Network Architecture



In the eThekwini Municipality, the distribution of the essential services such as electricity and water is largely dependent on the SCADA systems. SCADA systems use open standard protocols of which the description is available on the Internet. A SCADA system uses Internet protocols such as TCP/IP to transfer data, also runs on Linux or Windows operating systems as an application. SCADA systems are becoming vulnerable to hackers around the world. Security of SCADA is a challenge to the organisation. Contractors can connect to the SCADA network, Worm and virus scans are rarely conducted. Patches are not deployed and if deployed they are deployed late.

Most participants indicated the challenges often experienced when working on SCADA systems, and these included issues raised by various individuals from various business units. These were their individual views and not those of the department or unit.:

- No change management policy
- No network vulnerability testing conducted
- Lack of password policy
- No security awareness
- Lack of cyber-security policy
- Physical security threats such as vandalism and fire
- Hardware and software malfunctions due to various factors such as denial-of-service attacks, viruses, etc.
- Inadequate risk management processes
- Limited audit involvement
- Uncoordinated efforts amongst departments and units
- Poor support from senior management (sponsorship & buy-in).

Example of Water SCADA system destruction in South Africa

For 11 days, the citizens of Eersterust (Pretoria) and Mamelodi in Tshwane Metropolitan Municipality were left with no drinking water. This was caused by a damaged SCADA system in the reservoir due to vandalism. This happened in August 2006.

The controls that were highlighted to be important by the participants are the following:

- SCADA specific cyber-security policy. The municipality has an approved information security policy; however, participants indicated that the approved information security policy is biased towards ICT compared to PCS. This situation has led to ad hoc enactment of security measures. It is not known if security gaps exist or the right security measures have been implemented.
- Risk management approach. At senior management level, SCADA/PCS forms an integral part of risk management processes. This ensures that all information security aspects such as confidentiality, integrity, and reliability of SCADA systems, and business continuity planning are considered.
- Security awareness. Human element is one of key risk factors that needs attention in the cyber-security environment. Continuous security awareness keeps employees focused. Security aware employees assist to enhance the organisational security posture.
- SCADA systems and networks audit. The audit process provides assurance on the security of connections between networks and SCADA systems; security status of

distantly controlled and monitored sites; reporting security incident approach; and status of security relating to physical and logical access of SCADA components.

- Supply chain management policy to include SCADA systems. This enhances 24/7 availability of SCADA systems. Service providers and vendors have to be managed based on the SCM policy. After a disaster or malfunction, SCADA systems must be operating as soon as possible, and service providers could be part of the team to make the system functional again. Third parties must provide assurance that their employees are honest and reliable. Consultants working on SCADA systems must be supervised. Faulty equipment replaced by third parties may contain sensitive information. Sensitive information must be erased or the devices must be destroyed or sanitised before leaving the municipal premises.
- Defence in depth. SCADA networks are separated from corporate networks and from public networks. Accessibility of SCADA from other networks is a screen with no uncontrolled access able to take place. There are firewalls, separation of networks, and an authentication process. SCADA systems are not directly connected to the Internet.
- Controlled access to SCADA systems. Access to SCADA systems and networks is only available to authorised employees. It is controlled through electronic and physical controls.

Section 3: Information security

The IT unit has implemented cyber-security in the municipality, however; it has been done in a siloed approach. The controls implemented ensure that there is confidentiality, integrity, and availability of the data contained, and transmitted in the municipal ICT systems. The participants have indicated that IT personnel are competent to safeguard organisational information infrastructures. EThekwini Municipality has an approved information security policy. The custodian of this policy is the municipal IT unit. IT has been successful in the endeavours to implement an information security policy because the municipality has invested in both technical and social (human) resources. Municipal employees have to a large extent complied with the information security policy. This has been demonstrated by the internal audit reports, and reports from the office of the Auditor General.

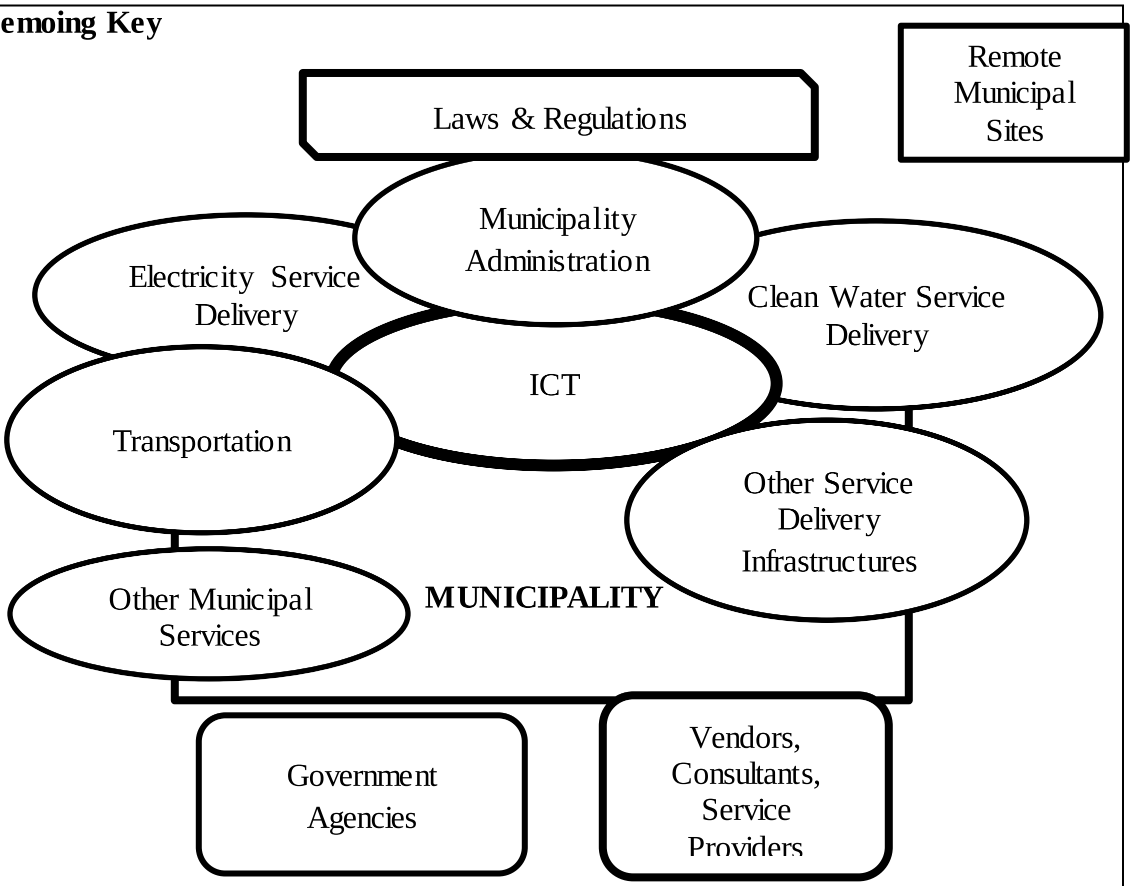
The municipality has implemented various technologies to safeguard information infrastructures. The municipality has also ensured that employees are aware of cyber-security risks facing the organisation. The municipality has provided employees with necessary skills and knowledge to implement information infrastructure protection mechanisms. In its endeavours, the IT unit has adopted industry best practices to safeguard organisational information infrastructures. Cobit is the IT governance framework that has been adopted in the municipality. The municipality has deployed technical tools to protect the organisational computer network. These tools include intrusion detection tools, network protection tools, network monitoring tools, and unauthorised access prevention tools.

Participants have indicated that IT governance takes place at senior management level in the organisation. The municipality has implemented an IT steering committee to provide leadership and direction on strategic IT initiatives. The IT budget is allocated based on the IT governance reports that are submitted to the IT steering committee. This committee meets at least quarterly. The IT steering committee monitors the implementation of the IT annual operational plan. The IT steering committee comprises senior management team members. Other cyber-security controls that have been implemented in the municipality include the following:

- Business continuity management (DRP)
- Access control to information infrastructures (both physical and logical)
- Network management
- ICT asset management (inventory management, maintenance, procurement)
- Computer networks vulnerability assessments
- Research & development on information security to understand current trends on cyber-security, and information infrastructure protection
- Software assets acquisition
- Segregation of duties
- Incident management
- Raising information security awareness
- Deployment of anti-virus software
- Individual performance management system

All these information security controls are applicable to cyber-security; however, they are only implemented in the ICT components. PCS also require similar to or more protection than the ICT counterpart. All the ICT security processes are included in the Service Delivery Budget Implementation Plan (SDBIP). Any other initiatives that are outside of SDBIP are not provided for in the budget and are not funded. The cyber-security initiatives must be included in the SDBIP in order to be successfully implemented. As a strategic goal, information infrastructure protection must be incorporated in the IDP in order to get the sponsorship it deserves.

Memoing Key


Remote Municipal Sites
Laws & Regulations
Municipality Administration
Electricity Service Delivery
Clean Water Service Delivery
ICT
Transportation
Other Service Delivery Infrastructures
Other Municipal Services
MUNICIPALITY
Government Agencies
Vendors, Consultants, Service Providers

Main issues raised by the participants

- There is lack of direction regarding the cyber-security in the organisation. There is no champion for cyber-security. This champion is supposed to facilitate and coordinate the efforts of safeguarding information infrastructures in the organisation. Various sectors within the organisation are safeguarding their sector-specific information infrastructures; however, this could lead to inconsistencies in the practices adopted to protect the vulnerable assets. Some sectors are more concerned about their core business and put in little effort for the protection of information infrastructures. This is more prevalent in the industrial control systems environment.
- The lack of cyber-security policy contributes to the uncoordinated efforts currently put into cyber-security. The roles and responsibilities are not clear in the execution of cyber-security. In as much as the ICT unit plays a role, it is a siloed role because other critical stakeholders are left out. The information security policy is not sufficient as it only focuses of ICT, while leaving out other sectors that have a role to play in cyber-security.
- Allocation of resources to safeguard the information infrastructure is not commensurate to the risk impact should the risk materialise. Allocation of cyber-security resources is not aligned to the value of the assets being protected. Some information infrastructures require control and monitoring 24/7, particularly those that support the critical infrastructures.

• The interconnectedness of information infrastructures compounds the problem of resource ownership and responsibilities, hence the protection thereof. These interdependencies create problems when planning and testing procedures for contingencies. One sector within the organisation has a disaster recovery in location X, another sector in location Y, and another in location Z. Due to interconnectedness, all these sites need each other in order to bring the information infrastructures up and running again. However, the siloed approach makes it difficult for all these sectors to consolidate their efforts to secure information infrastructures. • The inter-governmental relations on cyber-security and information infrastructure asset management is almost non-existent. Municipalities operate and own information infrastructures that support national critical infrastructures such as national airports, harbours, etc. Other spheres of government should be role players in the protection and risk management processes of these supporting information infrastructures.

4.4.3.1.2. Consolidated memoing for Question 2 initial coding

Table 4.8: Consolidated memo for Question 2 after the initial codes

Question: What methodologies are currently available to assess the cyber-security status in the eThekwini Metropolitan Municipality?
Objective: The objective of the question was to explore the methodologies currently employed to assess the cyber-security in the eThekwini Metropolitan Municipality.
The municipality has various committees to strengthen the governance processes in order to achieve the municipal mandate and objectives. Some of these committees exist as a result of statutory requirements such as Municipal Finance Management Act (MFMA). This committee is independent as its members are not employees of the municipality, nor are they councillors in the municipality. Audit and risk committee is one such committee that was formulated as a statutory compliance. The core function of this committee is to assess the adequacy and effectiveness of internal controls that management of the municipality has implemented to ensure that the municipality objectives are achieved, maintained, and enhanced. The internal audit committee advices Exco on risk management, and governance processes within the Municipality. Reporting to the audit and risk committee is the internal audit function. This is the audit that provides assurance services across the municipality processes. Amongst the components of the internal audit function is the ICT audit component which provides assurance on ICT processes across the municipality. The internal audit plan is approved by the audit and risk committee, and consulted with management before being implemented. In executing its function, the internal audit unit subscribes to industry best practices, and is guided by the prescripts for pertinent legislation and regulations. Industry best practices that have been adopted by the internal audit unit include the Cobit framework, and King IV report on corporate governance. Cobit guides the implementation of IT governance processes (protect IT assets, manage IT resources, alignment of IT to municipal strategic business objectives, etc.) King IV report on corporate governance

guides the municipality in adopting best practices when executing governance processes, risk management processes, and also IT governance processes. King IV report also provides guidelines on the mandates and composition of the audit committee. Assurance in the municipality is also provided by the office of the Auditor General of South Africa (AGSA).

Cyber-security is not the responsibility of one unit within the municipality. Cyber-security is the responsibility of all municipal business units that are using and or dependent on ICT in pursuit of their business unit's objectives. Most municipal business units are dependent on ICT. The dependencies vary per business units. Almost all departments are in the municipality play a role in cyber-security implementation.

Assessment is performed by auditors when they evaluate internal controls implemented in the municipality. Assessing cyber-security means evaluating processes/structures/relational mechanisms to identify whether cyber-security processes are adequate to safeguard the municipal information infrastructure. Assessing cyber-security includes processes to evaluate human behaviour towards information infrastructure protection. Assessment is conducted to identify if the environment is conducive to enhance the objectives of protecting information infrastructure protection.

As there is no known instrument to comprehensively assess the status of cyber-security in the metropolitan municipality environment in the country, the researcher requested the participants to identify how they would assess cyber-security in the municipality. What cyber-security processes and structures can be part of the assessment? The participants' responses include the following:

In the absence of cyber-security policy, information security policy can be used as a benchmark to assess cyber-security. Assessment of cyber-security enhances capacity development as the assessment processes identify the gaps in information infrastructure protection. Assessment of cyber-security enhances communication channels within the municipality as the assessment participants are given feedback to maintain and or improve cyber-security.

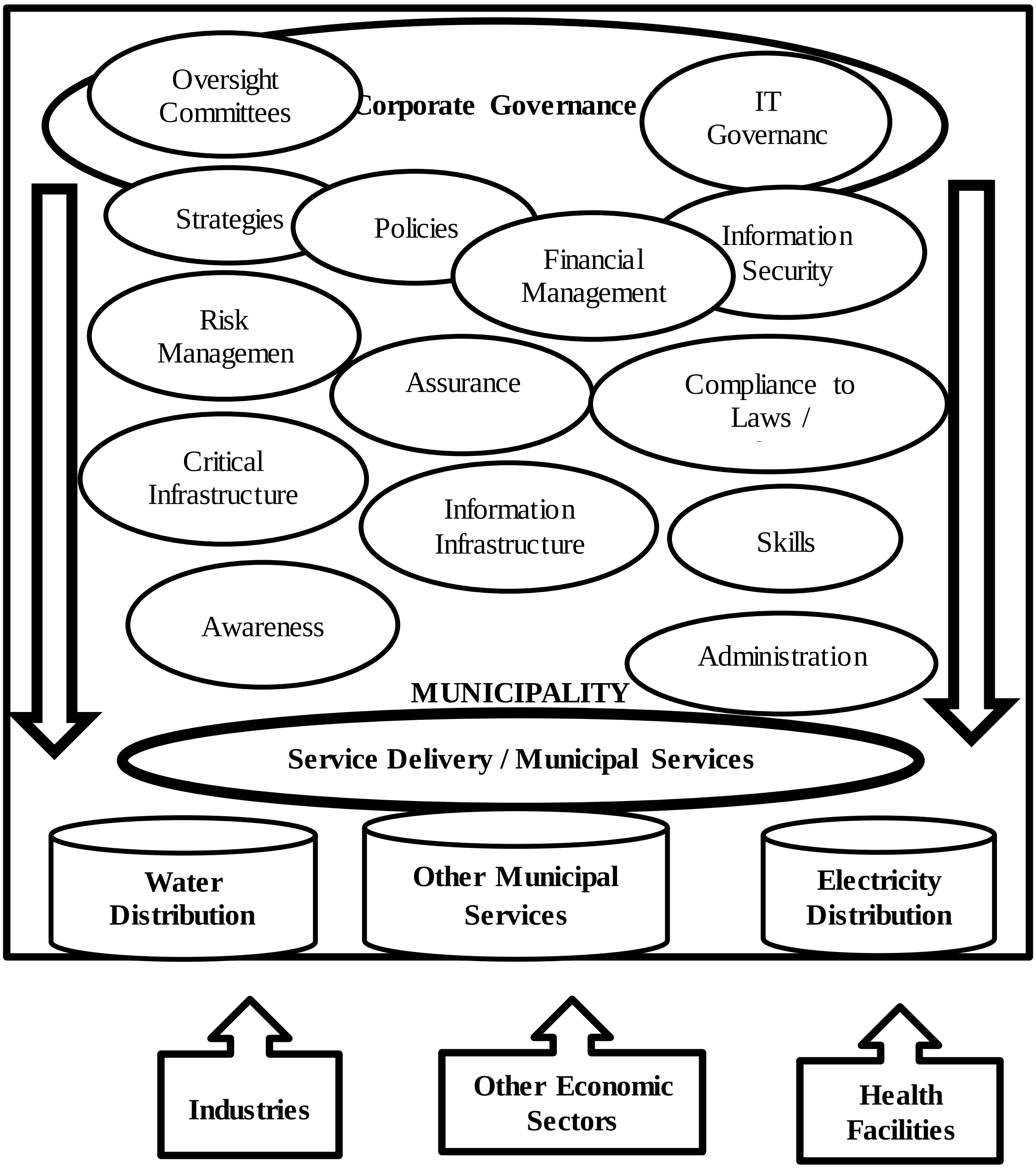
- Municipal governance processes are assessed through internal audit processes to determine if they cover cyber-security sufficiently. Governance processes include the various types of oversight committees.
- Various business units are conducting their own assessments through control of self-assessment processes. These assessments are conducted to identify gaps in their business processes. The intention is to strengthen their control processes.
- Internal audit function is also assessed for quality through the external quality review processes. But this assessment does not directly enhance cyber-security.
- Risk management processes are also assessed to determine if they adopt industry best practices. Risk management approach has been identified by the participants as one of the key areas that need to be evaluated to determine if they deal with cyber-security risks. Strategic risk register, for example, contains cyber-security as one of strategic risks that the municipality must mitigate.

- Top management commitment is assessed to determine the support the cyber-security programme receives from senior management in the municipality. Commitment from senior management can be in the form of sponsorship of various forms, i.e. sponsoring conferences dealing with cyber-security, sponsoring workshops, seminars, etc. Sponsorship can also include allowing employees to attend conferences, to join professional institutes, to attend user awareness programmes, etc.
- Assessment of information infrastructure acquisition is also essential. This includes processes such as SCM, contracts management, monitoring of service level agreements.
- Assess how the municipality is managing information infrastructure assets. This assessment includes identification of critical information infrastructure, maintenance, and disposal.
- Evaluate technical capacity to protect organisational information infrastructures. Technical capacity assessment encapsulates areas such as implementation of technologies that detect and prevent cyber-attacks. Technologies that are used to monitor computer networks and related devices. Physical protection of information infrastructures is also important to evaluate. Network vulnerability assessments are important monitoring and evaluation tools used by computer network custodians to assess security posture of organisational computer network. Security weakness identified during vulnerability assessments are rectified by management to ensure continuous protection of computer networks.

Cyber-security assessments can be grouped into various categories:

- Organisation category – which deals with assessing structures and processes that provide for the “cyber-security enabling environment” within the municipality.
- Technical category – deals with implementing relevant technologies and tools to effect the safeguarding of organisation information infrastructure.
- Human category – this is a social issue with deals with human beings who are operating the information infrastructures within the organisation. Third party service providers are catered for in this category.

Memo Conclusion



Key challenges identified by the participants

Cyber-threats to municipal infrastructure, and other assets, are amongst the sources of increasing concerns to policymakers in the municipality. Information infrastructures are now ubiquitous and components are interdependent wherein disruption of one component has a destructive, cascading effect on others.

- Cyber-security issues are not confined to ICT only but also involve physical threats to critical infrastructure. The current set-up to address the cyber-security challenges is not assisting the municipality as it should because 'the left hand does not know what the right hand is doing'. There are many cyber-security 'mini shops' in the municipality. There is no integration of activities, and if integration happens, it is by chance.

- The various business units that have responsibilities to secure their information infrastructures are not consistently adopting standards for information infrastructures categorisation that is aligned to levels of risk. As a result, is becomes a challenge to assess the capacity of the organisation to protection information infrastructure assets against cyber-threats. A holistic posture of cyber-security in the municipality could be a serious challenge to obtain due to disintegration yet working on interconnected and interdependent systems.
- There need to be checks and balances at a central point to ensure and certify that cyber-security implementation and assessment thereof are executed to strengthen the information infrastructure holistically. One cyber-security solution to a sector within the municipality can cause weaknesses (vulnerabilities) to other sectors due to interconnectedness. Assessing the status of cyber-security in a siloed manner could produce skewed outcomes if conducted in a ‘mini shop’ fashion.
- It is a challenge to determine if the overseeing that exists is assisting municipality efforts to provide risk-based, adequate, and cost-effective cyber-security. Sectors could be complying with various sector-specific legislation and regulations; however, with regards to cyber-security, there needs to a centralised assessment which should be conducted on an annual cycle.
- There is a lack of strategic understanding of the municipality’s cyber-security risk profile, including capacity of the workforce, and current threats. Municipalities are increasingly susceptible to cyber-threats due to the fact that their cyber defences tend to be less robust than other spheres of government.
- Users of information infrastructures are themselves threats to cyber-security. It therefore becomes essential for the municipality to assess how much users know about cyber-security. This assessment aims to strengthen controls around social engineering attacks. Also, the challenge here is about the fragmentation of the initiatives geared to address user awareness and training in the municipality. The depth of user awareness and training is not standardised across the municipality.

4.4.3.1.3. Consolidated memoing for Question 3 initial coding

Table 4.9: Consolidated memo for Question 3 after the initial codes

Question: How is eThekwini Metropolitan Municipality inculcating the culture of cyber-security across the organisation?
Objective: The objective of the question was to understand the processes that are employed to provide an enabling environment to develop, implement, and sustain a cyber-security culture across the organisation.

Cyber-security is the responsibility of all business units that operate and or depend on information infrastructure in pursuit of organisational objectives. A cyber-security culture can focus on various levels of the institution. These levels are as follows:

- Senior/Top management. This is the layer that drives corporate governance within the organisation. This layer sets the tone for all other layers in the organisation. This layer provides strategic direction to the organisation. It provides what to do, and how much has been budgeted for what has to be done. People participating on this layer are custodians of the IDP processes. This layer is a structure and the processes that are performed by the structure. At this level, cyber-security culture in the municipality is mainly influenced by:
    - the way things are done at a strategic level in the municipality
    - the personality of the municipality at a strategic level
    - what top management do to maintain, and in some areas enhance cyber-security in the municipality
- Business unit level. This the layer that implements cyber-security in the organisation. It is where technologies are deployed to safeguard information infrastructure. People participating on this layer are the technical experts who drive IDP implementation. This layer is made up of various structures and the processes that are performed by the structures. This structure provides actual delivery of services to the municipality community. At this level, cyber-security culture is mainly influenced by the following:
    - Nature of the business/operations that the unit conducts "*influence employee attitudes and have an impact on their behaviour*". What level of risk is the information infrastructure exposed to?
    - Nature of information infrastructure operated. "*Employees as members of a group/department*" are influenced by the nature of monitoring and auditing in the group.
    - Leadership of the various business units to "*to guide business units in making the right decision and to comply with Municipal policies*".
- Individual employee level. This is where human issues are considered. User training and awareness happen on this layer. Technical tools can be implemented to safeguard information infrastructure. However, if human issues are not addressed, the technical solutions that have been implemented will not function. Human issues for consideration include:
    - ethical behaviours
    - attitude towards cyber-security
    - cyber-security awareness
    - change management.

The domains under each level discussed are not mutually exclusive. In some cases there is and overlap of the levels. The participants indicated the following:

- Cyber-security culture is influenced by the tone at the top. Municipal executives show that they mean business by implementing policies and means to achieve those policies. A positive culture at executive management level motivates other tiers in the organisation to follow suit. Corporate governance culture on cyber-security is one element that cultivates the cyber-security culture across the municipality. Corporate governance includes internal auditing, risk management, and internal control.
- Cyber-security culture is influence by skill/training provided in the business unit as a group. Skills development can take many forms which include formal education through tertiary institutions, and occupational certifications through writing professional body examinations. Informal education is through collaborations with interested stakeholders within and external to the organisation, conducting workshops, seminars, breakfast sessions, etc. Strong leadership at business unit level has a positive influence on cyber-security culture in the municipality. Strong leadership will positively influence the cyber-security culture through enforcing asset management processes, contract management practices, cyber-security technical operations, and change management. Management reporting to various structures and committees also positively influences the culture of cyber-security in the municipality.
- At an individual level, a positive cyber-security mind-set inculcates the culture of cyber-security in the organisation. A positive mind-set is enhanced by programmes such as awareness campaigns, education, ethical behaviour, and attitudes. Ethical values are embedded in the organisational business processes. Automation of cyber-security processes enhances compliance and hence the positive culture. Monitoring of individual actions is one such enforcement control that ensures that users/staff are accountable for their actions online and on information infrastructures. Other factors that influence individual behaviours and attitudes towards cyber-security include individual performance management systems, rewarding of good behaviour and practices. Security breaches and non-compliance to policies are punished according to the severity of the breach/non-compliance. Making staff and users aware that their actions are logged by the systems and are monitored by management also has a positive influence on cultivating the culture of cyber-security in the municipality.

Key challenges identified by the participants

The municipality is a legislated institution. There are various laws that impact how the municipality operates and these include the Protection of Personal Information Act. The institution does not have an idea of how much has been done to comply with this act and any other acts impacting on information infrastructure.

- It is important to conduct continuous compliance, but there is no guarantee if those compliance tests cover all the areas that ought to be covered across the municipality.

- Reporting of cyber-security incidents is one factor that inculcates the culture of cyber-security. However, due to the lack of a centralised reporting centre, some attacks that have hit some areas in the municipality are not communicated to pertinent stakeholders inside the municipality or outside. The existence of reporting processes could be found in pockets across the municipality, but when this has occurred not every staff member was aware of what to do to report a cyber incident. Not every staff member is aware of how to identify a cyber-incident due to treating cyber-security in a siloed way. Therefore, there appears to be a need for the development of coordinated programmes to strengthen user awareness and reporting mechanisms. This coordinated reporting will cultivate the culture of cyber-security in the municipality. The positive culture could offer valuable insight in the municipality's preparedness to control cyber-security.
- Lack of cyber-security policy contributes to a poor cyber-security culture because there is no organisation-wide official stance on cyber-security. The presence of a cyber-security policy subsequently advances the compliance and enforcement processes. Without the official cyber-security it becomes a daunting task to preach the gospel of cyber-security in the organisation.
- Some form of contingency planning does take place in the municipality. However, simulations and various tests conducted do not generate scalable results to inform strategy and policy development. Continuous assessment of contingency plans inculcates the culture of cyber-security in the municipality, but only if the efforts and outputs are appropriately coordinated and directed.
- Continuous cyber-security assessments either through qualitative or quantitative approaches seek to produce structured results that are measurable. These assessments however only inculcate cyber-security culture if the results inform municipal cyber-security strategy implementation, and form the basis for budgetary allocations regarding cyber-security.

4.4.3.2. Focused coding

The researcher never lost sight of what the enquiry wanted to achieve. The research sought to determine the cyber-security status in South African metropolitan municipalities. The codes that were identified during the initial coding process were aligned with the research intentions. After the initial coding had been done, focused coding was conducted, and that was in alignment with the ConGTM. During the focused coding phase, the codes from the initial coding were more directed, selective, and conceptual than for the initial coding. During this phase, the researcher synthesized and explained larger data segments. Most significant and frequent codes were identified; however, the researcher had to make decisions about which initial codes made the most analytic sense to categorise the data incisively and completely.

Municipality develops and implements the IDP.	IDP is the service delivery framework in the municipality.	Various business units participate in research and development activities.
Unit heads implement the municipal vision.	Each business unit manages its own cyber-security affairs.	Adoption of ICT is the underlying cause of cyber vulnerability.
Unit heads implement municipal strategies.	ICT unit communicates information security policies across the organisation.	Collaboration on cyber-security amongst various departments takes place.
Business units encourage their staff to attend seminars and breakfast sessions normally hosted by professional institutes.	Management provides budget and prioritises skills development for employees working on information infrastructures.	Composition of cyber-security steering committee is made up of senior management officials responsible for delivery of essential services.
ICT is the core of information infrastructure.	Senior management team has developed cyber-security steering committee.	Cyber-security steering committee should develop cyber-security policy.
External independent assessments are conducted on the security of information infrastructure assets.	Units that have implemented PCS have established 24/7 computer networks monitoring centres.	Formulate central point for addressing and coordinating cyber-security municipal-wide.
Various business units are conducting health checks on the information infrastructures.	Office of the Auditor General conducts audits on information infrastructures.	Investment on cyber-security projects/implementations is monitored and reported on.
Municipality has formulated a technical working group on cyber-security whose composition includes both streams of ICT and PCS.	The basis of business processes is to deliver services to the local citizens.	Cyber-security policy encompasses all information infrastructures beyond IT unit.
IDP is the service delivery framework in the municipality.		

Integrated Development Cyber-security

- Various business units
- Integrated Development plan
- Coordination of efforts
- Facilitation of cyber-security
- Custodian of cyber-security
- Alignment to service delivery
- Centralised coordination
- Policy development
- Continuous assessment
- Cyber-security steering committee
- Continuous development
- Continuous monitoring
- Continuous reporting
- Collaboration
- Assurance

Figure 4.4: Formation of focused code: Integrated development cyber-security

Day-to-day highest decision making is delegated to Exco.	Municipal administration requires ICT support.	Exco delegates policy development to the municipal manager.
Municipal council is the highest decision-making body.	Municipal Systems Act guides the implementation of performance management systems.	Senior management has developed a portfolio responsible for strategic assets management.
Municipality comprises various functional domains.	Municipal manager leads the senior management team.	Senior management has developed a supply chain management policy.
Senior management has implemented risk management processes across the organisation.	Water and sanitation is an essential service provided.	Senior management team develops and continuously maintains strategic risk register.
Municipal manager leads the municipal administration processes.	MFMA guides the establishment of internal audit function.	Expenditure is linked to the IDP which is reviewed annually.
IDP is the service delivery framework in the municipality.	Exco delegates policy development to the municipal manager.	Infrastructures committee provides oversight on municipal infrastructure assets.
Unit heads implement municipal strategies.	Corporate governance is guided by the King IV report.	Management of finances is guided by MFMA.
Information infrastructures support business processes in pursuit of service delivery.	Governance processes are executed by senior management team.	Through IT governance processes, ICT has adopted industry best practices such as Cobit.
Finance committee provides oversight on municipal finances.	Municipal manager reports to Exco.	Critical infrastructures are supported by information infrastructures.
Audit committee provides oversight on the governance processes that management has implemented.	Various business units develop and submit for approval their annual budgetary requirements.	

Cyber-security Governance

- Formulate municipal strategy (IDP)
- Provide direction in the organisation
- Provide leadership
- Provide sponsorship
- Steer the municipality to comply with laws and legislation
- Drives organisational culture
- Implement corporate governance as guided by industry best practices
- Implement oversight committees
- Set the tone
- Set the right culture
- Implement IDP
- Setting oversight structures
- Continuous reporting
- Setting regulatory framework

Figure 4.5: Formation of focused code: Cyber-security governance

Office of the Auditor General conducts audit on information infrastructures.	Audit committee approves the internal audit annual operational plan.	Various business units conduct contingency plans testing.
MFMA guides the establishment of internal audit function.	Internal audit function provides assurance on the implementation of IT governance processes.	Internal audit function provides assurance on the municipal performance information.
Business units that own PCS deploy technologies to monitor, detect, and prevent unauthorised access to their computer networks.	Audit committee provides oversight on the internal controls that management has implemented to mitigate the identified risks.	Control weaknesses identified during the audit process are communicated to senior management for subsequent rectification of those controls.
ICT unit deploys technologies to monitor, detect, and prevent unauthorised access to organisational computer networks.	Audit committee provides oversight on the internal risk management processes that management has implemented.	Audit committee provides oversight on the governance processes that management has implemented.
Unit heads provide methodologies to safeguard organisational assets guided by pertinent policies, legislation and regulations.	Senior management has implemented risk management processes across the organisation.	Independent consultants are engaged to test compliance to pertinent IT laws and regulations.
External independent assessments are conducted on the security of information infrastructure assets.	Internal audit reports are communicated to the audit committee to maximise accountability.	Cyber-security steering committee approves cyber-security implementation plan.
Unit heads are responsible for the functional/operations effectiveness of their business units.	Audit committee approves the three year risk based rolling plan.	Audit on IT system is conducted by internal audit unit.
Various business units are conducting health checks on the information infrastructures.	Unit heads develop and maintain their respective operational risk registers.	Governance audits are conducted to assess the effectiveness of governance structures and processes.

Cyber-security Assurance

- Implement internal audit function as guided by MFMA
- Conduct compliance audit
- Focus audit plan on high risk areas
- Audit function report to audit committee
- Internal control deficiencies are communicated to management
- Enforce alignment to IDP
- Conduct assurance
- Hold management accountable
- Conduct risk assessments
- Focus on high risk areas
- Approve assurance plan
- Assess internal controls
- Evaluate risk mitigation strategies
- Conduct compliance

Figure 4.6: Formation of focused code: Cyber-security assurance

Various business units provide essential services.	Senior management has developed a portfolio responsible for strategic assets management.	Critical infrastructures are supported by information infrastructures.	**Manage Information Infrastructure** • Identify critical information infrastructure • Formulate information infrastructure catalogue • Implement asset management • Secure information infrastructure • Conduct risk assessment on information infrastructure • Adopt industry best practices in managing information infrastructure • Provide assurance on the controls implemented to protect information infrastructure
Senior management has implemented risk management processes across the organisation.	Unit heads provide methodologies to safeguard organisational assets guided by pertinent policies, legislation and regulations.	Business units that own PCS have developed and implemented their infrastructure maintenance plans.	
Legal unit has identified relevant legislation and regulation pertaining to information infrastructures.	ICT unit has developed and implemented IT assets maintenance plans.	Management provides budget and prioritises skills development for employees working on information infrastructures.	
Various forms of infrastructure are other services provided.	Cyber-security policy encompasses all information infrastructures beyond IT unit.	Breach of security is communicated to the process and information infrastructure owner.	
Employees' ethical behaviour is one of the factors to consider when addressing protection of information infrastructure.	Electricity SCADA system is an example of PCS.	Various units adopt industry best practices to achieve consistent results on their business objectives.	
Access to information infrastructure is restricted to only authorised employees, consultants, and service providers.	Various business units are conducting health checks on the information infrastructures.	Supply chain management processes include vendor/supplier management practices.	
Municipality has formulated a technical working group on cyber-security whose composition includes both streams of ICT and PCS.	ICT and the data therein are the underlying causes for cyber vulnerability.	Remote access to organisational information infrastructure assets is controlled.	

Figure 4.7: Formation of focused code: Manage information infrastructure

Cyber-security policy encompasses all information infrastructures beyond ICT Unit.	Cyber-security policy to extend from information security policy.	Senior management has implemented risk management processes across the organisation	**Cyber-security technical operations** • Deploy tools, technologies and methodologies to secure information infrastructure • Prepare for cyber-incidents • Monitor tools deployed to safeguard information infrastructure • Implement cyber-security policy • Allocate resources to protect information infrastructure • Promote knowledge generation on cyber-security • Protect information infrastructure assets • Detect vulnerabilities • Control access to information assets • Monitor user activities on information infrastructure
Breach of security is communicated to the process and information infrastructure owner.	Formulate central point for addressing and coordinating cyber-security municipal-wide.	ICT unit plans/design corporate/organisational telecommunication networks.	
Access to information infrastructure is restricted to only authorised employees, consultants and service providers.	ICT unit conducts continuous computer networks vulnerability assessments.	Systems documentation including user manuals are developed and maintained.	
ICT unit has implemented network perimeter control on corporate networks.	Uploading of software to the organisational information infrastructure is restricted to authorised employees.	Various business units have implemented segregation of duties control.	
Software development methodology is prescribed for system testing before implemented to live environment.	Remote access to organisational information infrastructure assets is controlled.	ICT unit provides guidelines on the complexity of IT system users' passwords.	
Operating systems default passwords are controlled.	Collaboration on cyber-security amongst various departments takes place.	Tertiary education institutions partner with various business unit on cyber-security related matters.	
Users are made time-out if there is inactivity for a specified amount of time in a session.	ICT unit communicates the computer network statistics to various business unit heads.	Disaster recovery plans for information infrastructures are continuously tested.	
Control weaknesses identified during the audit process are communicated to senior management for subsequent rectification of those controls.	Unit head provides methodologies to safeguard organisational assets guided by pertinent policies, legislation, and regulations.	ICT unit deploys technologies to monitor, detect and prevent unauthorised access to organisational computer networks.	

Figure 4.8: Formation of focused code: Implement cyber-security technical operations

Employees' ethical behaviour is one of the factors to consider when addressing protection of information infrastructure.	Individually employees sign the Internet use policy.	Access control processes include an authentication mechanism.
Internet usage is monitored.	Various business units are monitoring compliance with the acceptable use of information infrastructures.	Systems documentations including user manual are developed and maintained.
Individual employees are encouraged to attend relevant professional conferences in order to understand current trends on cyber-security.	Individually employees sign the e-mail use policy.	Commitment by employees to protect information infrastructures is essential.
Conduct user awareness workshops.	Comply with HR policies and procedures.	Perform vetting exercise before confirming employment.
Send employees to training and development.	Conduct breakfast sessions to empower users and operators of information infrastructures.	Conduct social engineering assessments.
Promote affiliations to professional institutes.	Conduct performance assessment in alignment with pertinent policy.	Communicate cyber-security policy across all the employees.
Include cyber-security on induction programmes.	Before joining the employ of the municipality, employees are vetted in terms of qualifications and previous work experience.	Various business units conduct skills development for their employees.
Educate end-users on cyber-attacks, including social engineering.	Access to information infrastructure is restricted to only authorised employees, consultants and service providers.	Employees are made aware of the consequences on breach of cyber-security policy.
Systems logs are generated and checked by responsible officials.	Trustworthiness of employees working on information infrastructures is a serious consideration.	Various business units encourage staff to get certified in their various occupations.

Human Issues on Cyber-security

- Encourage cyber-security knowledge management
- Conduct user awareness
- Conduct research and development
- Provide systems user manual/guidelines
- Promote staff ethical behaviour
- Implement users' accountability on protecting information infrastructure

Figure 4.9: Formation of focused code: Manage human issues on cyber-security

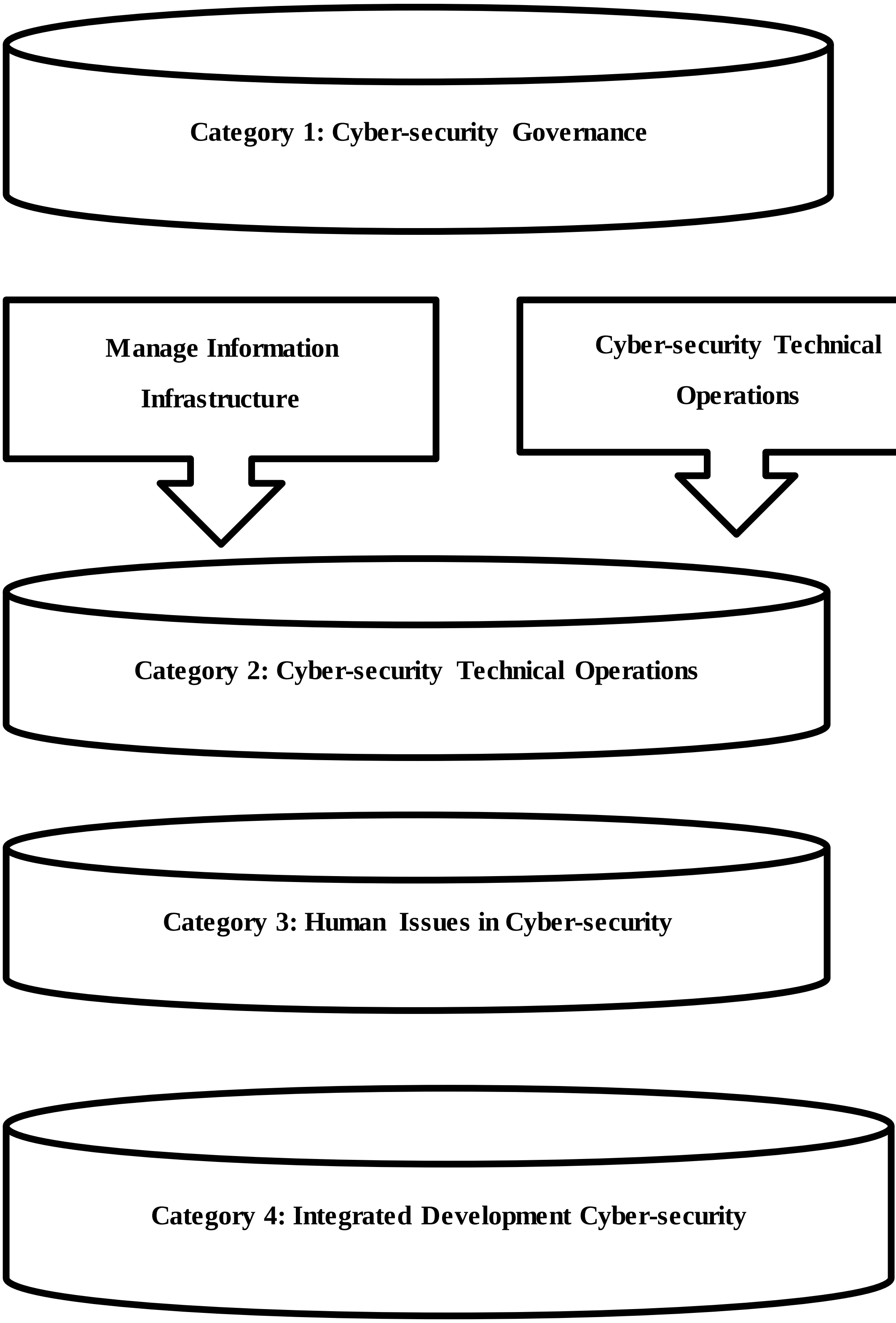

Category 1: Cyber-security Governance
Manage Information Infrastructure
Cyber-security Technical Operations
Category 2: Cyber-security Technical Operations
Category 3: Human Issues in Cyber-security
Category 4: Integrated Development Cyber-security

Figure 4.10: List of categories from focused codes

Category: Cyber-security governance memoing

It is important to justify how certain codes were grouped to formulate codes. That justification was developed through the utilisation of memo writing. The King III report (2009) posits that good governance is about effective leadership that rises to challenges. Effective leadership provides direction in a business situation, defines strategy, and establishes the ethics and values to guide behaviour and practices within the organisation. The respondents identified governance as one of the critical success factors for effective implementation of cyber-security within the municipality. Through governance practices, senior management develops strategies and policies to ensure that the direction taken does activate the mandate and organisational objectives. The metropolitan municipalities have a mandate entrenched to the Constitution of the country. The core mandate of each municipality is to provide service delivery to the citizens. Delivery of services includes the provision of electricity (energy), water and sanitation, transportation and other essential government services. The municipality through governance processes must ensure that services that are essential for daily lives of the citizens are provided. Governance processes entail:

- setting and steering strategic direction of the municipality;
- providing oversight of the municipal strategy implementation;
- approving policies to steer municipal strategy direction; and
- ensuring accountability through reporting and disclosures.

Municipal council is ultimately accountable for cyber-security governance. The day-to-day municipal governance processes have been delegated to Exco. The administration of the municipality is delegated to the City Manager. Governance processes set the tone and culture in the municipality. In ensuring that there is continuous delivery of these essential services, through governance processes, the municipality must ensure that strategies are put in place to safeguard the information infrastructures that these essential serves are dependent upon. Through effective governance processes, the municipality should develop a cyber-security strategy and policy that will guide the protection of information infrastructures within the municipality. Participant 3 said "*Senior Management in the municipality must illustrate leadership in managing cyber security and model the behaviour expected of employees*". The same sentiments were echoed by Participant 7 who said "*The senior management of the organization should establish a cyber-security policy which is appropriate to the* *organization's business objectives. The policy should define cyber-security objectives or a framework for setting the same*". Participant 10 contended that "*Leadership and governance on cyber-security is critical for successful implementation of cyber-security strategy across the municipality*". Cyber-security governance provides an environment that is conducive to implement cyber-security and subsequently securing critical information infrastructures that are essential for service delivery. The activities that are undertaken in the cyber-security governance include the following:

- Sponsoring cyber-security through providing of adequate funding. Participant 13 said "*Executive management involvement must be clear in implementing cyber-security strategy".*
- Setting effective oversight committees to monitor cyber-security implementation. Participant 6 emphasised that *"At a governance level, an oversight committee must be implemented to impose accountability and reporting on cyber-security. This accountability would strengthen the protection of information infrastructures against cyber threats".*
- Fostering cyber-security accountability through continuous reporting. Participant 25 said "*Other governance processes are continuously reported on at various structures in the municipality. These processes include Financial Reporting, Disclosures, Performance Information, etc.*"
- Formulating and supporting effective guardian of governance processes. Participant 4 said "*Internal audit must operate according to the prescripts of MFMA, and industry best practices such as King IV report on corporate governance. Internal Audit annual operational plan must include all types of audits based on the high risk areas*".
- Formulating and supporting enterprise-wide risk management processes. Participant 10 said "*The risks associated with cyber-security are colossus and therefore the treatment for cyber-security risks must be dealt with at a very high level of the Municipality. Cyber-security risk is a municipal strategic risk which affects business continuity*".
- Formulating and supporting the Municipal Integrated Development Plan (IDP) to which the cyber-security strategy is aligned. Participant 18 said "*Executive Management must develop municipal's ability to secure information infrastructures*

> *that are relevant to achieve strategic objectives which is the IDP. The ability to protect information infrastructure improves cyber incident response, cyber crisis management, redundancy, and enhance critical infrastructure protection resilience".*

Generally corporate governance refers to the system by which an organisation's processes are directed and controlled, in the pursuit of achieving business objectives. If the municipality is paying attention to safeguard stakeholders' interests which is the core of corporate governance, then cyber-security must be part of the focus areas in corporate governance processes.

Category: Integrated development cyber-security memoing

Cyber threats are a serious concern to municipal authorities and hence they cannot be left to an individual person or a single business unit within the organisation. Cyber-security impacts almost every business unit in the municipality. The interconnectedness of information infrastructures warrants that every business unit that forms part of the interconnectedness be part of the team to deal with cyber-security. The risks associated with cyber-security are huge and could have devastating consequences should they materialise. Cyber-security risks are highly likely to happen and the possible impact could include non-delivery of essential services to the citizens. The municipality monitors and controls some service delivery processes through the industrial control systems (ICS) which often reside inside critical infrastructures like power plants, power grids, and water distribution. These ICS use ICT in order to function as intended. Due to inter-dependencies amongst systems, failures of ICS have a cascading impact in other systems. Participant 3 said "*The municipality should implement a long-term plan for cyber-security*". Cyber-security strategy is an important element in addressing the cyber-security challenges in the municipality.

The intention of this research was to assess the cyber-security status in the metropolitan municipalities. An assessment was conducted through benchmarking against a given yardstick. A strategy is one of the yardsticks to assess how far the organisation has gone towards reaching the intended destination as outlined in the strategy document. Participant 10 confirmed the essential role of cyber-security strategy in the organisation when he said "*In order to report on cyber-security, we shall need to devise and implement cyber-security strategy from which to develop targets that should be reported on continuously*". Cyber-security policy cannot be separated from the associated cyber-security strategy. Cyber-security policy present guidelines on what must be done and not done to achieve the organisational endeavours to implement a cyber-security strategy. Cyber-security policy must, amongst other things, explicitly specify what information infrastructures have to be protected and against which threats. Cyber-security policy offers recommendations on the roles and responsibilities in implementing cyber-security strategy. Participant 6 said "*Cyber-security status can only be measured if there is a cyber-security policy in the municipality*". Participant 17 concurs this view when saying "*Cyber-security strategy and cyber-security policy should be developed, implemented, and published for implementation in the municipality. Once implemented, they will be used as a benchmark to test compliance against*".

Due to the interconnectedness of information infrastructures in the municipality, it is essential to establish a central point to coordinate and facilitate measures to safeguard information infrastructures from various cyber-threats. The central point will offer coherent synergy among all stakeholders in pursuit of secure, safe, and resilient information infrastructure for municipal critical sectors. The central point is a nerve centre that seeks to integrate common industry best practices/controls that are universal to all the information infrastructures. Each sector within the municipality, however, will advance their own best practices for the protection of their respective information infrastructures. The nerve centre will advise the management of the critical sectors about the manpower, infrastructure, skills, and strategies required to advance the protection of their respective critical information infrastructures. The controls to protect information infrastructures will be updated occasionally by the nerve centre to keep in tune with emerging technologies and related protocols. The programme will consult and collaborate with all the stakeholders through workshops, feedbacks, discussions, trainings, and regular interactions. The nerve centre will consult domain experts on the continuous protection of information infrastructure. The cyber-security central point aims to conduct and pursue measures, including raising information security awareness and conducting cyber-security associated research and development for the protection of the information infrastructure in the municipality. The activities that are undertaken in this domain include the following:

- Planning and delivering municipal cyber-security policy and strategy that are aligned to the municipal IDP. Participant 14 said "*Cyber-security strategy is crucial to mainstreaming cyber-security programme across the Municipality because it helps prioritise cyber-security as an important policy area. Cyber-security strategy and* *policy determines responsibilities and mandates of cyber-security programme, and guides provision of resources to the emerging and existing cyber-security issues and priorities".* Participant 1 said "*In order to successfully implement cyber-security in the municipality setting, there must be an existence of an overarching programme for cybersecurity coordination, including a coordinating body with a consolidated budget*". Participant 19 said "*Municipal cyber-security strategy content must explicitly link municipal risks, priorities, and objectives such as critical information infrastructure protection, and cyber incident response capacity".*

- Encouraging cyber-security knowledge across the municipality. Participant 2 said "*The municipality must implement minimum competencies applicable to all businesses units that operate information infrastructures. Minimum competencies includes qualifications, certifications, and awareness of cyber threats*".

- Rolling out and prioritising resources to implement cyber-security strategy across all the municipal units. Participant 21 said "*There must be an existence of a designated structure or unit within the Municipality that is responsible for cyber-security mitigation strategies which include detection, prevention, and prepare for contingency situations".*

- Building municipal-wide cyber-security capacity. Participant 6 said "*The municipality must implement centrally managed effective widespread use of cyber-security technology to protect municipal information infrastructure. This centralised approach will encourage the implementation of cyber-security standards and good practices".* Participant 12 confirmed this view when saying "*There is a need to build cyber-security capacity starting from information infrastructure procurement procedures to software development processes".*

- Assessing cyber-security status in the municipality. Participant 9 said "*The cyber-security nerve centre must assess the status of cyber-security to subsequently enhance the safeguarding of municipal critical information infrastructures. Cyber-security various stakeholders within the municipality must be assessed on their roles and responsibilities executed to implement or sustain cyber-security. The role of Executive Management, departments, and other actors must be constantly assessed to identify the gaps in the protection of information infrastructures*".

- Setting of standards and technologies to secure information infrastructures. Participant 13 said *"There must be a cyber-security framework that is built around industry best practices, and must include governance controls, technical security controls"* Participant 20 also says "*A function within the municipality must prescribe the adoption of industry best standards. There must be collaborative work through risk management practises to minimise the impact and likelihood of cyber-security threats*".

The Municipal Systems Act put IDP at the centre in entrenching principles for local government development. Cyber-security is key to service delivery because the interconnectedness of ICT and PCS support the delivery of services as recorded in the IDP. Embedding cyber-security in the IDP is intended to formalise and elevate cyber-security processes so that they are given priority and commitment from all key stakeholders within the municipality.

Category: Cyber-security technical operations memoing

The core mandates of a metropolitan municipality are to provide service delivery to the people in the jurisdiction of the municipality. There are essential services provided by the municipality to the citizens and these include electricity and clean water. For the municipality to survive, there must be proper administrative support provided. There are mission critical computer systems that support the day-to-day running of the municipality. In order for the municipality to provide essential services, it must be able to collect rates and other monies due to it.

Electricity distribution and water distribution by the municipality are dependent on 'smart systems' such as industrial control systems such as a SCADA system. These 'smart systems' exist in cyberspace because they are operated remotely through the use of intelligent devices such as computers, servers, sensors, networks and related software. Therefore, all the 'smart system' components are critical information infrastructures. These critical infrastructures operate or work with information – hence they are called critical information infrastructures.

Essential services are referred to as critical services, and the infrastructures that support these critical services are referred to as critical infrastructures. The information infrastructures supporting the essential/critical services are known as critical information infrastructures. Critical information infrastructures include computer networks, servers, software, computer applications, technologies and hardware, all which support the critical infrastructures in the municipality. CIIs are largely impacted by cyber-security. CIIs are those computer-related assets the incapacitation or destruction of which, shall have devastating influence on municipal well-being, security, the economy, public health or safety. Therefore in order to provide the needed cyber-security to CIIs, the municipality needs to know what IIs it has. It becomes important that the municipality develops an inventory or a register of all information infrastructures.

Through a holistic approach, each information infrastructure custodian should take all necessary measures to facilitate protection of IIs, and this can be achieved through coherent coordination, synergy and raising information security awareness among all stakeholders. It is at this level where IIs are safeguarded from unauthorised access, modification, use, disclosure, disruption, incapacitation or destruction. The implementation of the protection controls has largely been driven by the availability of an approved information security policy and IT governance model employed by the ICT unit. Participants in this study highlighted that technologies such as firewalls, anti-virus tools and access controls (both logical and physical) have already been implemented in their areas. However, these technologies have been implemented in a siloed approach and hence there is no proper coordination of implemented activities to address the cyber-security challenges.

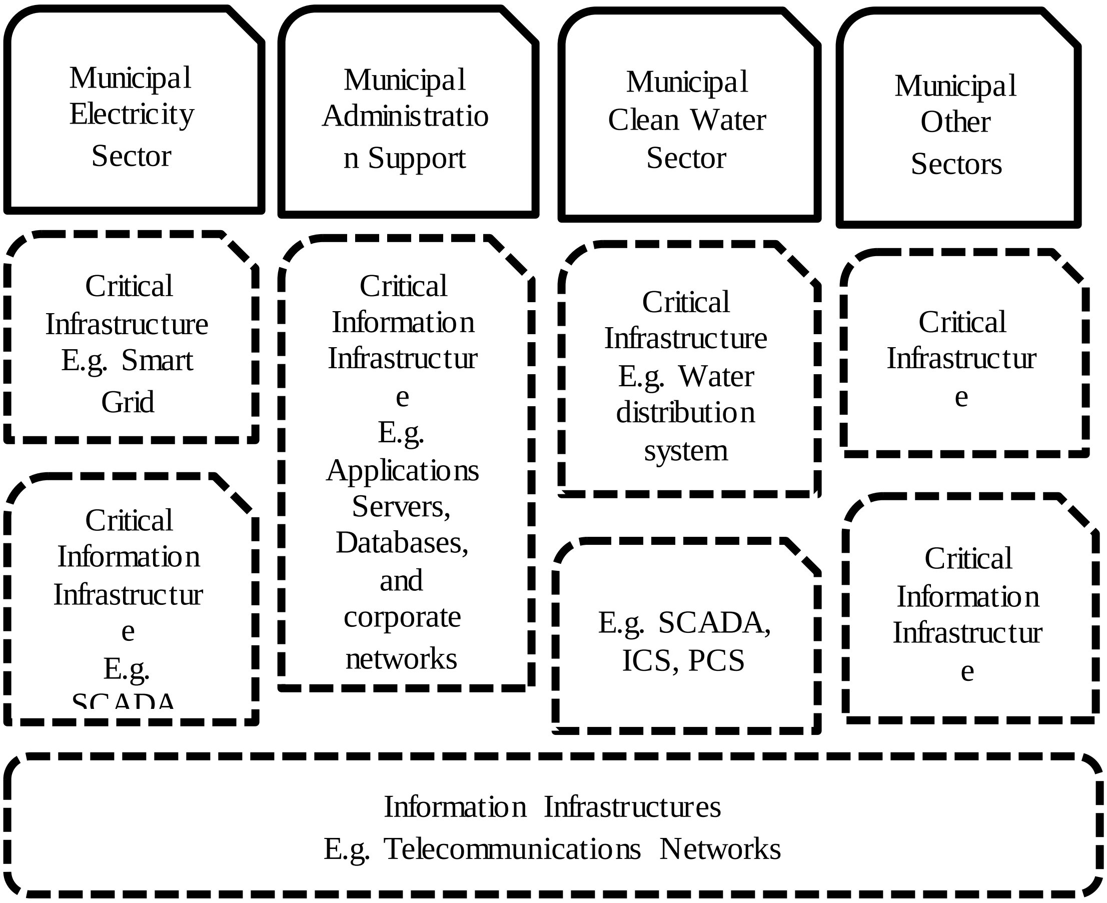

Municipal Electricity Sector
Municipal Administration Support
Municipal Clean Water Sector
Municipal Other Sectors
Critical Infrastructure E.g. Smart Grid
Critical Information Infrastructure E.g. Applications Servers, Databases, and corporate networks
Critical Infrastructure E.g. Water distribution system
Critical Infrastructure
Critical Information Infrastructure E.g. SCADA
E.g. SCADA, ICS, PCS
Critical Information Infrastructure
Information Infrastructures E.g. Telecommunications Networks

Figure 4.11: Linking critical information infrastructures to critical infrastructures

The entirety of inter-connected intelligent devices, computers and networks, and the essential information flowing through them is termed information infrastructure. ICS are part of the information infrastructure family as they use intelligent devices through telecommunication services to control and monitor the industrial processes. Security incidents in information infrastructures are mainly due to a mixture of technological and organisational weaknesses. The information infrastructure that supports critical municipal processes becomes a critical information infrastructure purely because the critical infrastructures it supports are essential for the well-being of people and the municipal economic prosperity. Information infrastructures have become vulnerable to cyber-attacks. They are susceptible to threats exploiting software vulnerabilities such as operating systems, protocol implementation, and application. Information infrastructure requires protection from disruption; unauthorised modification, disclosure, access, and use. Various controls are used to safeguard information infrastructure in the municipality.

Cyber-security operations are the activities performed in order to protect information infrastructures from cyber-ills, and or to limit the impact should cyber-attack take place. These activities include: implementation of information security policy, controlling access to information infrastructure, user identification and authentication, controlling and monitoring systems administrators' privileges, implementing cyber-security incidents' response procedures, implementing network perimeter protection, conducting network vulnerability and penetration testing, implementation of information infrastructure maintenance plans, preparing for contingencies, implementation of assets and inventory management, security certifications, adoption of industry best practices, disposal of information infrastructure, vendor security and outsourcing, network device protection, hardware and software hardening, hardware and software testing, conducting of periodic audits (for assurance), implementing mechanisms for data/information protection, implementing physical security to information infrastructure, and conducting risk assessments. Protection of information infrastructures against cyber ills includes deploying technologies, tools and methodologies in pursuit of securing the assets.

Participant 7 said "*Cyber security program should provide the required confidentiality, integrity and availability (CIA) protection to the information assets of the organization*".

Participant 20 said "*Municipality must strengthen capacity to detect, and defend against cyber-attacks. Both technical security controls and human must be deployed to secure information infrastructures*".

Category: Human issues in cyber-security implementation

The first line of defence against cyber-attacks is well-trained staff. Cyber-security awareness and pertinent training assist in the reduction of cyber-security breaches and the related possibility by providing well-intentioned staff with the knowledge to avoid becoming inadvertent attack vectors for instance by unintentionally downloading malware. It becomes essential that the municipality establishes and maintains a cyber-security awareness programme that is robust to ensure that information infrastructure users are alert and responsive to the importance of guarding sensitive information and the risks that are associated with it. Cyber-security operations go hand in hand with user management. Operations address the technical components of cyber-security implementation. User management on the other side addresses soft issues on cyber-security implementation including user awareness campaigns. In as much as the municipality has invested heavily in technical controls to protect its computer systems and data, most of these controls can be rendered useless when staff lack cyber-security awareness training.

Municipal staff members have access to internet and online activities. This exposure to the Internet significantly increases cyber-related risks to the organisation. Some of the activities performed by employees that are considered to be risky include not protecting sensitive information stored on, or transmitted from, their computers, and opening suspicious e-mails. User management initiatives include coordinated/facilitated sessions with the employees about good cyber-security practices. Through these awareness sessions, it is anticipated that employees will understand that they play a crucial role in safeguarding the organisation's information infrastructure assets. Activities conducted in this category include the following:

- Educating information infrastructure users on cyber-threats. Participant 21 said "*While understanding the technological approaches including hacking tools and defence in depth are important countermeasure mechanisms, a cultural approach is necessary to control the human element which makes the selected technological approach a viable measure".*
- Informing users of their responsibilities to safeguard information infrastructures. Participant 26 said "*All users should receive regular refresher training on cyber-security, information and human security risks relevant to their particular sectors' information assets"* Participant 2 echoed this sentiment when saying "*Employees must sign consent on the acceptable use of organisational applications and related information. Before each employee is granted access to computer system, the employee must acknowledge read and understood security requirements and compliance thereof*".
- Training employees who provide technical skills on protecting information infrastructures. Participant 29 said "*Employees that support or operate information infrastructure are appropriately trained to ensure that Municipal information assets are always confidential, there is information integrity, and information is always available when required to authorised users*". Participant 31 confirmed this view when saying "*Industry specific certifications are essential when supporting information infrastructure and related facilities. Security personnel be certified information security managers, Network practitioners / specialist must be certified network engineers*".

- Providing continuous skills development to enhance protection of information assets. Participant 23 said "*Employees must know current trends on how to operate and protect information assets. Employees must be members of professional bodies, and to sustain their membership, they must continuously attend to relevant conferences and various sessions organised by the professional bodies*". Participant 25 said "*Individual performance assessments are conducted with the aim of enhancing skills development to strengthen safeguarding of information assets*".
- Enforce cyber-security policies at an individual level. Participant 11 said "*The municipality must constantly conduct compulsory information sharing sessions with the users to refresh them on cyber-security policy. These compulsory session must be conducted during on-boarding of employees, and on an annual basis at a minimum*".
- Inculcate cyber-security culture, through enforcement, monitoring, and evaluation. Participant 1 said "*Access to information infrastructure is controlled even to legitimate users. Activities of legitimate users are recorded to keep the logs of events, and users are made aware when granted access to information assets*" Participant 4 said "*Management continuously monitor network activities in order to detect and prevent illicit activities to gain access to information assets*" Participant 24 said "*There are various types of ICT audits that are conducted to evaluate the adequacy and effectiveness of controls implemented to secure information infrastructures*".
- Punishing cyber-security breaches and violations. Participant 8 said "*Management monitor activities on information infrastructures. The intention of monitoring is to ensure that network users continuously operate within the ambits of the Municipal information security policy. The details of the users that are found to be transgressing the policy are communicated to the owner of relevant information assets impacted by the transgression*".

This category is mainly responsible for driving a cyber-security culture through the understanding of cyber-related risks in the municipality. Activities in this category involve complying with the Protection of Personal Information Act. This category enforces users' understanding of personal information protection online. Through this category, cyber-security is prioritised and embedded in the values, attitudes, and practices of the users across the municipality. This category encourages a cyber-security mindset which fosters attitudes, values, habits and practices of employees individually, and other actors in the cyber-security ecosystem that increase the resilience of users to cyber. Reporting of cyber-security breaches is encouraged through this category. It is through this category where users of the Internet are prepared with the capability to identify non-legitimate websites (including impersonation attempts), and have a sense of control over providing personal information online. Individual employees are provided with the ability to assess the risk in using information infrastructure services, including the cyber-security environment and constantly adjust their behaviour based on their assessment.

4.4.4. Theoretical coding

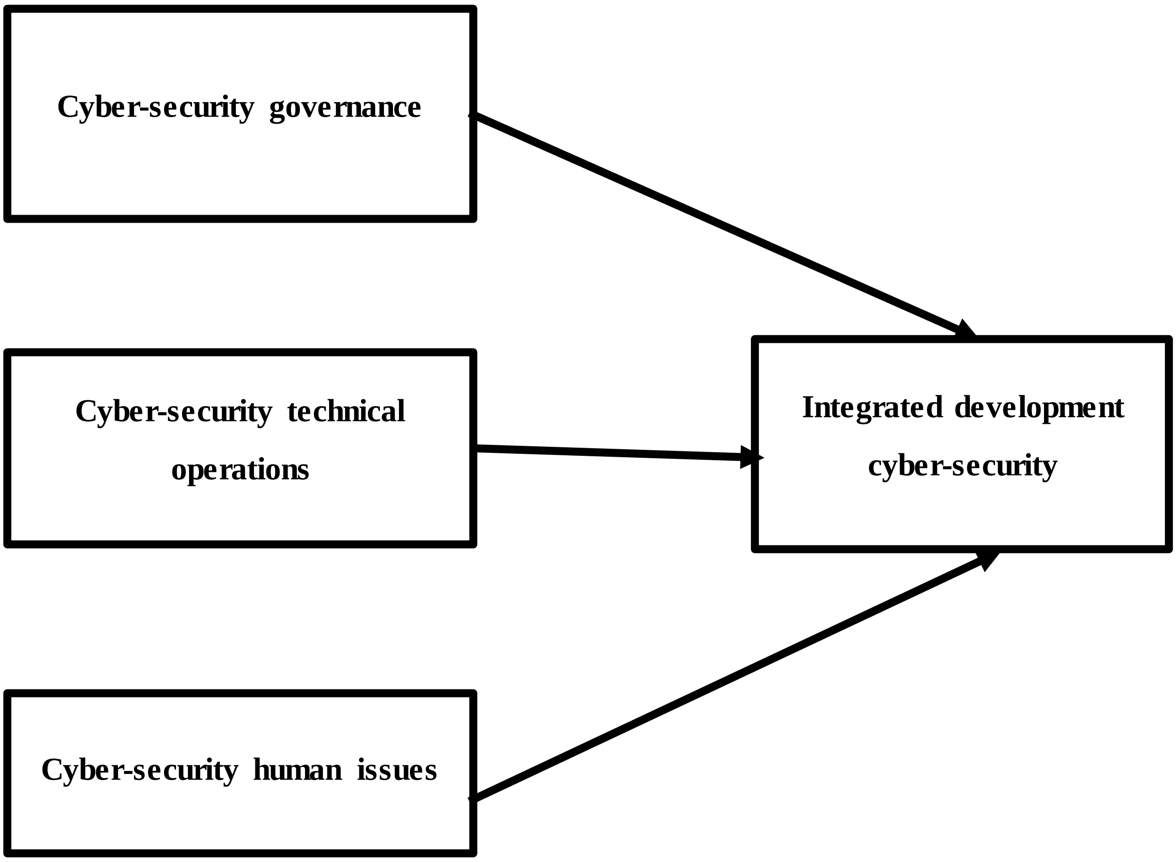

Cyber-security governance
Cyber-security technical operations
Cyber-security human issues
Integrated development cyber-security

Figure 4.12: Linking of focused codes

The researcher recognised the need for a representation of the interrelationships between categories that would aid the development of theoretical explanations, and subsequently adopted the conditional relationship guide developed by Scott (2004). The conditional relationship by Scott (2004) suggests building a matrix to understand the relationship among categories by asking investigative questions of *what, who, when, where, how, and with what* *result of consequence* (Scott, 2004). The researcher adopted the conditional relationship matrix guide as described in the following table.

Table 4.10: Relationship matrix

"What is the category?"
"Who impacts on the category?"
"When does the category occur?"
"Where does the category occur?"
"Why does the category occur?"
"How does the category occur?"
"With what consequence does the category occur or is the category understood?"

Core category: Integrated development cyber-security

This category ensures that singular municipal cyber-security posture exists, and is a designated municipal body to disseminate and consolidate feedback on the cyber-security strategy across the municipality to constantly improve the municipal cyber-security posture. Guided by the changing risk assessments, the programme will have the ability to reassign tasks and budgets dynamically. The three categories of cyber-security governance, cyber-security technical operations, and cyber-security human issues are all linked to the integrated development cyber-security category. The core category is the centre for the municipal cyber-security capacity through the formulation and delivery of the cyber-security strategy. This category enhances municipal cyber-security resilience through input from governance, technical operations, and management of human issues.

What is the category about?

The category is about consolidating the efforts implemented for cyber-security. It ensures that the municipal cyber-security strategy is linked explicitly and directly to municipal objectives, risks, priorities, as well as the development agenda of the municipality. This category seeks to align the cyber-security strategy to municipal integrated development. Cyber-security supports the municipal mandate of service delivery. In the municipality context, allocation of resources to implement municipal development programmes is aligned to the service delivery budget implementation plan. The allocation of financial resources to support cyber-security implementation is linked to the service delivery budget implementation programme. IDP is a strategic plan for the municipality and hence aligning cyber-security to the strategic plan invites the attention of the executive management of the organisation. Senior management sets the tone at the top regarding organisational culture. Positive cyber-security culture at the executive management level filters down to cyber-security technical operations, and cyber-security human issues.

How does this category achieve what it does?

The category can achieve to be the cyber-security nerve centre through proactive, frequent revision and improvement of the municipal cyber-security strategy to adapt to the ever changing technology environments and threats. The municipal cyber-security strategic plan must align with municipal strategic priorities, drive investment in security, and drive capacity building for securing information infrastructures. The cyber-security programme performs monitoring processes, collects measurements and relevant metrics and data with the aim of determining trends to inform a decision-making process. At the centre of cyber-security, the strategy should be to raise awareness, mitigate cyber-risks, establish and sustain cyber-incident response competence and safeguard critical infrastructures.

The alignment is achieved through the involvement and commitment of executive management. Senior management provides leadership in the organisation. Executive management leads the entire organisation, not just the business unit. Risk management's approach to service delivery is one of the key drivers that aligns cyber-security to the IDP (strategic plan). ICT and other information infrastructures support the delivery of services to the municipal community. Cyber-risks have the potential to interrupt the provision of service delivery due to the interconnectedness of the service delivery infrastructure to information infrastructures. Information infrastructures are susceptible to cyber-risks. Cyber-security as a mitigating action to cyber-risks enhances the possibilities of uninterrupted service delivery to the municipal citizens. Cyber-security is an enabler of efficient municipal service delivery.

Who are the role players in this category?

The role players in this category include the executive management members who are the custodians of information infrastructures and those that their critical infrastructure depend on the information infrastructure By default, the ICT unit is a member and key role player. Executive management is responsible to implement governance processes in the municipality. By virtue of being part of the executive management, business unit heads are also role players. Business unit heads drive the implementation of the IDP, and subsequently the technical implementation of the cyber-security operations.

When does the category take place?

Integrated cyber-security takes place during the strategy-setting process in the municipality. This category is a risk mitigation action against continuity of service delivery risk. As an enabler to service delivery and municipal administration processes, ICT and information infrastructures must be protected against cyber ills. This category also takes place during cyber-security technical implementation at various business units.

Where does the category occur?

This category takes place across the organisation; however, it promotes a central point that is responsible to coordinate the cyber-security efforts. Through the implementation of the tools and technologies to protect organisational information assets, this category also takes place at business unit level across the impacted functional areas in the municipality. Through the use of IT systems, users at all levels in the municipality are impacted because they have an obligation to safeguard organisational assets including information and technology assets. User awareness and education take place at an individual level across the municipality.

Why does the category occur?

This category occurs to align cyber-security to the organisational strategic framework which is the IDP. The alignment focuses on key initiatives, projects, and strategic programmes that achieve the legislated municipal mandate. The alignment also links cyber-security to the municipal performance management tools and budget. The alignment forms the basis for cyber-security monitoring and evaluation. The integrated development cyber-security category does not only focus on what the cyber-security programme does to safeguard information infrastructure, but also how the cyber-security programme's activities are planned and implemented municipal-wide. Integrated development cyber-security is an instrument for the integration and coordination of cyber-security planning, implementation, and monitoring.

What are the consequences of implementing this category?

Vulnerabilities and cyber-security requirements in critical infrastructure supply chains are evidently recognised, recorded and managed. The consequences of implementing this category are: creation of effective integrated-cyber-security strategy and policy; delivering municipal-wide defence and resilience competency; maintaining the benefits of a cyberspace vital for the municipality; and centralised management and coordination of cyber-security efforts. Integrated development of cyber-security ensures that the developed cyber-security strategy and policy cover all the relevant functional areas within the municipality. The basis to allocate cyber-security resources to cyber-security implementation mechanisms is transparent as it is aligned to IDP. The category enhances consistency in the implementation of cyber-security across the municipality as the various business units are involved. Integrated cyber-security strengthens coordinated efforts in addressing cyber-security challenges. It provides a centralised hub for cyber-security knowledge. This category enhances the critical infrastructure protection competencies.

Cyber-security governance category

What is this category about?

This category is about providing leadership and governance in the municipality. This is achieved through strategy and policy development. The category provides the road map to implement strategies to achieve the municipal mandates of service delivery. Managing cyber-risks is one of the mechanisms employed to enhance the achievement of service delivery.

How does this category achieve governance?

This category is achieved through the adoption of industry best practices such as the King IV report on corporate governance. Also, compliance with regulations is essential to achieve cyber-security governance. There are various committees established to participate and enhance governance. The committees ensure oversight on cyber-security implementation initiatives. An audit committee is formulated in compliance with MFMA. The audit committee provides assurance of the internal control, risk management processes, and governance implemented in pursuit of organisational objectives. Strategy formulation and setting direction through policy development contribute significantly to cyber-security implementation across the municipality.

Who are the role players in this category?

Executive management members are the key role players as governance processes are their core functions and obligations. Various municipal committees also provide oversight in the implementation of cyber-security. These committees include Exco, and the audit committee and portfolio committee for municipal infrastructure. The audit committee holds management to account for the control weakness identified. The infrastructure committee ensures that service delivery is not disrupted. This is achieved through the monitoring of the support processes supporting the service delivery infrastructures. The monitoring is through risk management practices.

When does the category take place?

Cyber-security governance is a continuous process as it is part of corporate governance. The activities that are reported to executive management and various portfolios are normally reported quarterly. For example, the audit committee reports to Exco quarterly. This category takes place when reporting on cyber-security takes place. Reporting can be driven by the audit committee's reports, portfolio committee's reports, cyber-security steering committee's reports, etc. During the processes of assessing strategic risks, the cyber-security governance process is embedded in the strategic risk management process.

Where does the category occur?

Cyber-security governance processes take place at an executive level in the municipality. The cyber-security strategy and policy development occur at the organisational leadership level. At strategic level, the integration, coordination, and alignment of various strategies take place.

Why does the category occur?

This category occurs to provide the direction that the organisation takes on implementing the cyber-security programme. The category provides leadership, and epitomises the cyber-security programme to the municipal IDP. The allocation of resources to support the cyber-security programme is decided at this level (category). This category takes place to elevate cyber-security to an executive management level for sponsorship and related support.

What are the consequences of implementing this category?

Implementing cyber-security governance leads to coordinated efforts is dealing with cyber-risks. The executive management team is responsible for organisational strategy and policy development. The cyber-security strategy and policy provide the direction that the organisation takes to address cyber-risk. Cyber-security governance strengthens the efforts made to protect the municipal information infrastructure. The involvement of the executive management team promotes opportunity for alignment between the municipal IDP and cyber-security strategy. This category is responsible for providing funding, i.e. allocation of resources to cyber-security implementation. Cyber-security governance provides an enabling environment for all other categories to take place.

Cyber-security technical operations category

What is this category about?

It is about implementing the municipal cyber-security strategy guided by the policy. Strategy and policy are developed by the cyber-security governance team (executive management). This category is about deploying tools and technologies to safeguard the organisational information infrastructure against cyber-risks. The cyber-security operational team ensures that service delivery takes place by protecting the critical information infrastructures.

How does this category achieve its objective?

There are interdependencies in the information infrastructure environment, and this interconnectedness has strategic effects on the well-being of the municipality. Collapse or destruction of information infrastructures has serious consequences. Attack on II could lead to blocking or disrupting the municipality communication, impede the circulation and distribution of energy/electricity, water, and other important services delivered by the municipality. Driven by risk management processes, various business units ensure protection of the information infrastructure against cyber-risks. The protection mechanisms include the utilisation of industry best practices to monitor, detect, and prevent illicit activities in the computer networks. Industry best practices such as Cobit are used to guide implementation of IT governance which is an important proponent of cyber-security. The mechanisms that are implemented to safeguard information infrastructures include access controls (physical and logical) network protection tools and technologies, IT asset management, risk management, business continuity, networks vulnerability assessments, etc.

Who are the role players in this category?

Various business units and functional groups are key role players to effect the protection of information infrastructures. Custodians of information infrastructures are the ones who ensure that their assets are protected and functional to achieve the objectives of the municipality. The role players are groups/departments who depend on information infrastructures to deliver services. Assurance providers also participate in this category as they test if the controls implemented to protect ICT assets are functioning as intended by management.

When does the category take place?

Cyber-security technical operations take place on a day-to-day basis. Information infrastructure assets need protection 24/7. Cyber-security technical operations implement processes that aim to continuously safeguard IT assets across the municipality.

Where does the category occur?

This category occurs at business unit level (groups, departments). The actual deployment of technologies to protect information infrastructure assets thus takes place at business unit level. ICT is the custodian of information security in the municipality. HR is the custodian of human resources and development programmes. Various business units who are the custodians of service delivery processes such as electricity and water are involved. These business units facilitate the implementation of cyber-security programme in their respective functional areas.

Why does the category occur?

The category occurs to deploy the technologies and tools to protect the organisational information infrastructure against cyber-threats. Information infrastructures support other infrastructures in the municipality. This category therefore occurs to ensure that there is uninterrupted support provided by information infrastructures to those other critical infrastructures. This category supports and protects the interconnectedness of information infrastructures.

What are the consequences of implementing this category?

Cyber-security operations implement controls to safeguard information infrastructure assets in the municipality. Uninterrupted service delivery is achieved because protection of support systems, such as information infrastructures is provided. Critical information infrastructures are identified. Protection of information infrastructures is commensurate with the priority of services supported by the infrastructure. Compliance with relevant legislation and regulations is achieved.

Human issues in cyber-security category

What is this category about?

The first line of defence against cyber-attacks is well-trained staff. Cyber-security awareness and pertinent training assist in the reduction of cyber-security breaches and any related possibility by providing well-intentioned staff with the knowledge to avoid becoming inadvertent attack vectors.

How does this category achieve its objectives?

To protect information infrastructure, employees need to know the use and value of the infrastructure being operated. The employees need to understand the cyber-risks, and their potential impact on the functioning of the information infrastructure being used, and the organisational impact should the risk materialise. User awareness and education mechanisms are important in this category. Individual performance management processes are key to ensure that employees are performing as expected, and that they possess the requisite skills and capacity to protect organisational information infrastructure assets. Skills development is aligned to the strategic objectives of the municipality.

Who are the role players in this category?

The role players are the individual employees. Each employee has an obligation to safeguard organisational assets. Through the performance assessment process, management determines the capacity of each employee to protect information infrastructure assets. Management also plays a role in providing the needed resources to achieve skills development, education, and awareness campaigns. Various business units such as human resources, ICT, and internal audit have roles to play.

When does the category take place?

User and employee activities take place on a day-to-day basis. User awareness is driven by the ICT department, and the custodians of the information infrastructure assets. User awareness also takes place during new employees' induction process and the HR department gets involved. When conducting employee performance assessments, skills gaps are identified and training is provided based on the gaps identified.

Where does the category occur?

This category takes place at an individual level across the organisation. Each employee working on protecting the information infrastructure is provided with appropriate skills to execute the protection function competently. Users of information infrastructures are sensitised and educated on the risk associated with cyber environment. The enforcement of the cyber-security policy takes place in this category. Individual user activities on information infrastructure are logged and monitored. Where a user has violated the security policy, they face punitive measures.

Why does the category occur?

This category occurs to ensure that individual employees are competent to handle and protect organisational information infrastructure assets. Users are made aware of cyber-security risks. Users are educated in the "do's and don'ts" when working on municipal information infrastructure. Skills and capacity to execute information infrastructure safeguarding duties are continuously upgraded to move with current trends on cyber-security.

What are the consequences of implementing this category?

Cyber-aware employees strengthen the protection of IT assets against cyber-risks. An employee with appropriate skills who supports the information infrastructure enhances the protection of information infrastructures. Skills development is directed because it is based on an individual performance assessment exercise. Cyber-security implementation becomes successful if everyone who works with information infrastructure is able to play a role in protecting information assets against cyber-risks.

4.5. CHAPTER SUMMARY

Chapter 4 provided a background on the research site which is eThekwini Metropolitan Municipality. This municipality is the only Category A Municipality in the province of KZN. The rationale for selecting this municipality was provided. The process followed to conduct the empirical study was discussed. Research ethical clearance was obtained from the UKZN research office before the empirical study could be initiated. Semi-structured interview questions were developed and discussed. ConGTM processes to analyse the data were presented. The researcher followed the data collection and analysis process based on the ConGTM. Data collection took place at the same time as data analysis. Comprehensive interviews were conducted with the participants who were purposively selected based on the research objectives. Interviews were transcribed and initial codes were formulated. Through the memoing process, the initial codes were analysed further and focused codes were developed. Focused codes were further analysed through the memo-writing process. Theoretical coding took place following the focused coding process. Focused codes were theoretically linked together through a memoing process and conditional relationship as developed by Scott (2004).

CHAPTER 5
THE EMERGENT THEORY

5.1. CHAPTER INTRODUCTION

Chapter 5 discusses the process of the theory of *integrated development cyber-security* emergent. Table 5.1 presents the structure of this chapter.

Table 5.1: Structure of Chapter 5

	Topic	**Overview**
5.1	Chapter introduction	Presents chapter outline.
5.2	How the theory emerged	Discusses how ConGTM was used to develop the theory.
5.3	The dependent construct	Discusses the theory main construct.
5.4	The independent constructs	Discusses the theory secondary constructs.
5.5	Chapter summary	Presents highlights on sections covered in the chapter.

5.2. HOW THE THEORY EMERGED

ConGTM was adopted to conduct the research. Through semi-structured interviews, data was collected and in parallel analysed. Two coding processes were followed and these were initial coding and focused coding. In between these two coding processes, there was a memo-writing process in which data was analysed and context provided for such analysis. After the two coding processes, theoretical coding started and the focused codes were linked together into a coherent unit. The researcher was an active participant during the data collection process. The researcher was able to apply his mind to interpret and put into proper context some of the responses that were provided by the participants. Figure 5.1 presents the steps the researcher undertook to develop the theory of *integrated development cyber-security*.

It is important to highlight that the research main objective was to determine the cyber-security status of metropolitan municipalities in South Africa. The GT study was conducted to determine how cyber-security can be assessed.

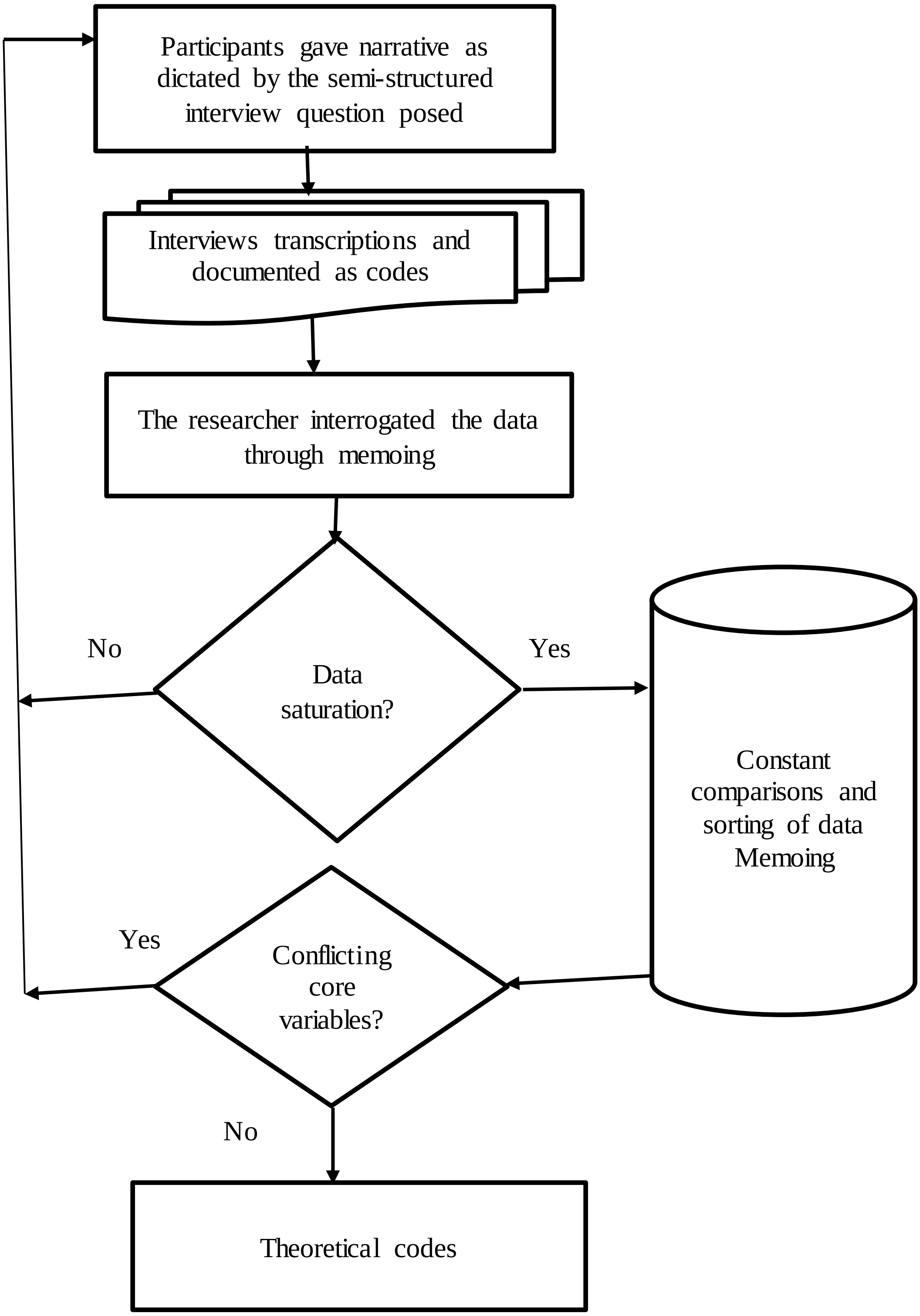

Participants gave narrative as dictated by the semi-structured interview question posed
Interviews transcriptions and documented as codes
The researcher interrogated the data through memoing
No
Data saturation?
Yes
Constant comparisons and sorting of data Memoing
Yes
Conflicting core variables?
No
Theoretical codes

Figure 5.1: Process in which the theory was developed

The researcher had to formulate GT research questions in order to determine how to assess cyber-security capacity. Initial codes and subsequent focused codes were created. The data collected was in a narrative form that warranted comprehensive interrogation by the researcher. The narratives did not provide answers at face value. The researcher had to carefully apply the ConGTM to analyse the data.

The research participants provided narrative responses to semi-structured interview questions, and such narratives for example included that from **Participant 3** "*Appropriate Senior Management involvement in the Municipality cyber-security initiatives provides the enabling environment for all other cyber-related activities*". Another example was from **Participant 11** "*The composition of cyber-security committee includes all senior management team who are responsible for the delivery of essential services to the citizens. These managers have authority to commit organisational resources in cyber-security implementation".* These narratives, together with others, put forward the account that actions are needed to form the basis, and motivate and strengthen the safeguarding of municipal information infrastructure from cyber-security threats. The narratives by the participants did not immediately reveal that *Integrated development cyber-security* is the cornerstone for successful cyber-security implementation in the municipality. The researcher was able to identify from the participants' responses that four focus areas were key to assess the cyber-security status holistically across the municipality.

Through the memoing processes, the researcher interrogated the data to determine what kinds of questions needed to be posed to subsequent participants' interviews. At some point during the data analysis process, the researcher reached a point when participants kept revealing similar sentiments, and that was when data saturation occurred. Guided by the research objectives, when data saturation materialised, the research ceased to collect data since latent meanings had been unearthed from the data already collected.

Theoretical coding linked various codes in as logical way possible. This linking of different codes was made possible by memoing processes at various stages of data collection and the analysis phases. Various memos exposed the low level of descriptive data such as that from **Participant 14** "*Cyber-security processes are conducted in a siloed fashion. People from process control automation believe their systems are secured because their telecommunication networks are isolated from the corporate computer networks*". Similar narratives were observed from **Participant 17** who said "*Most employees believe cyber-security belongs to IT unit, forgetting that everyone has a role to play. Some municipal business systems are used by almost every employees, such as e-mail system, and internet.*

These users are not from IT Unit but across different functional areas within the Municipality". Through data analysis processes, the researcher could extract the meaning attached to solve the issues highlighted by these narratives to mean *Integrated development cyber-security* is necessary for successful cyber-security implementation, and subsequent continuous assessments thereof.

Through constant comparisons of different codes and memos, particular theoretical codes emerged. These theoretical codes conceptualised the relationships amongst various codes for resolving the research problem of what specifically needs to be the focus areas when assessing cyber-security status. Most of the participants highlighted in their narratives that they were aware of what the ideal cyber-security assessment entails. Through data interrogation it became clear that participants were doing the following:

a. Emphasising the linking of cyber-security to the Municipal Integrated Development Plan; centrally coordinating and facilitating the protection of information infrastructures across the municipality; and development of cyber-security nerve centre to update policies and strategies as guided by the metrics and current trends in cyber-security and information infrastructure protection.

b. Highlighting the involvement of the senior management team to provide leadership, direct, formulate and approve cyber-security strategy and policy. Executive management is accountable regarding the delivery of municipal services to the local community. Any disruption to service delivery is a serious concern to executive management. Cyber-security risk is one serious threat to the service delivery mandate. Cyber-security risk mitigating actions must be sponsored and supported by executive management in every possible way.

c. Highlighting the importance of deploying and monitoring appropriate tools and technologies to protect information infrastructure against cyber-risk. Automated safeguarding technologies and tools are implemented to continuously protect and monitor information infrastructures.

d. Emphasising the need for critical consideration of human issues on cyber-security implementation. Implementation of excellent automated security tools alone does not guarantee total protection of information infrastructures. Humans are the first line of defence in protecting the municipal information infrastructure.

The adoption of ConGTM processes guided the discovery of the latent subject. This subject existed although it was not possible to extract it without ConGTM of two phases coding and the embedded memo writing activities. The ConGTM revealed this latent subject, with the dependent variable called *Integrated development cyber-security*. *Integrated development cyber-security* was the dependent variable because it took into account most of the variations in the data collected. The researcher picked up through data interrogation that *Integrated development cyber-security* was the mechanism that was constantly chosen by the participants to resolve their main unease of "*siloed fashion, lack of organisational direction, and co-ordination*" on strengthening cyber-security implementation in the municipality. One valid account on which *Integrated development cyber-security* grounded theory that has emerged from this enquiry could be evaluated is to determine whether it is a vigorous consistent hypothesis on which the participants repeatedly attempt to resolve their uneasiness of "*siloed fashion, lack of organisational direction, and co-ordination"* of cyber-security implementation in the municipality. All three identified independent variables have an impact on the "*Integrated development cyber-security*" dependent variable.

5.3. THE CORE CONSTRUCT

The research identified *Integrated development cyber-security* to be the dependent construct which is the core construct in this study. The study participants were based in eThekwini Metropolitan Municipality. They had to resolve the issue of "*siloed fashion and lack of organisational coordination and direction*" to successfully implement cyber-security in the municipality. The researcher defined the *Integrated development cyber-security* core construct as follows:

> Embedding cyber-security processes in the municipal IDP with the aim of unifying all cyber-security initiatives to strengthen and cultivate information infrastructure protection against cyber-risks. In other words, what is required to successfully implement and assess the cyber-security status in the metropolitan municipality? The answer that this research came-up with is *Integrated development cyber-security* that epitomises the municipal IDP.
>
> *Integrated development cyber-security* promotes integration and coordination of cyber-security activities that are centred on the municipality strategic objectives.

- The participants indicated that *Integrated development cyber-security* is positively influenced by the appropriately functioning cyber-security governance in the municipality.
- The participants indicated that *Integrated development cyber-security* is positively influenced by the appropriately working and coordinated cyber-security technical operations.
- The participants highlighted that *Integrated development cyber-security* is positively influenced by the adequately managed cyber-security human issues.

The researcher identified the constructs of the *Integrated development cyber-security* dependent construct. These constructs include:

- centrally coordinated and directed cyber-security initiatives;
- aligning cyber-security to IDP to support allocation of resources;
- conducting cyber-security research and development to enhance cyber-security knowledge;
- centralised protection of municipal critical information infrastructure;
- centralised development and updating of cyber-security strategy and policy;
- integrated cyber-security assessments;
- integrated setting of industry best practices and cyber-security framework;
- integrated implementation of contingency plans due to interconnectedness of information infrastructures;
- facilitating collaborations with various actors in cyber-security; and
- unified management of supply chains involving critical information infrastructures.

5.4. THE THEORY CONSTRUCTS

The researcher identified three independent variables that influence the core (dependent) construct.

Independent construct: Implement appropriate cyber-security governance

Good working cyber-security governance ensures that:

- there is a cyber-security strategy, and that there are resources to achieve the strategy objectives;
- there is an approved cyber-security policy, and that there are resources to achieve the policy objectives;
- the cyber-security strategy is in alignment with the municipal strategic framework which is IDP;
- there are municipal oversight committees performing the oversight function in the cyber-security programme;
- the executive management team provides the required leadership to drive the implementation of the cyber-security programme throughout the municipality – tone at the top is important to cultivate the cyber-security culture;
- compliance with relevant legislation and regulation takes place;
- risk management processes include cyber-security risks;
- independent assurance is provided over cyber-security processes that have been implemented to protect the information infrastructure;
- consequence management is performed in cases where there is poor/inadequate implementation of internal controls to mitigate cyber-risks – also in cases where there are breaches or violations of security on the information infrastructure; and
- there are directed and coordinated efforts across the municipality to implement the cyber-security programme.

Independent construct: Cyber-security technical operations

Cyber-security technical operations implement and deploy tools, methodologies, and technologies to protect information infrastructures. Competent cyber-security technical operations ensures that:

- information infrastructure assets are protected against cyber-risks;
- the right technology is deployed to secure municipal telecommunication networks;
- critical information infrastructures are identified and protected;
- there is a catalogue of the critical information infrastructure;

- industry best practices are adopted in the protection of information of the infrastructure;
- continuous monitoring and evaluation of the implemented controls are in place to protect information infrastructure;
- acquisition of the information infrastructure follows organisational supply chain management processes;
- appropriate management of vendors and consultants – this includes management of service level agreements to ensure continuous provision of support to municipal critical information infrastructures;
- there is centralised management and coordination of the cyber-security programme – information security functions with the ICT unit which is the custodian of information security across the organisation; and any information security mechanisms are centralised in this function; and
- appropriate management of information infrastructure assets is in place.

Independent construct: Human issues in cyber-security

Implementing good technical controls to protect information infrastructures on their own does not guarantee information infrastructure protection. Human beings that work on information infrastructures make it possible that the implemented technical controls are operating as intended. Appropriate management of human issues on cyber-security ensures that:

- employees are provided with skills and knowledge to protect information infrastructure;
- employees are encouraged to be affiliated to pertinent professional institutes;
- there are individual performance management systems to assess the competency of employees;
- adequate budget is provided to implement user awareness programmes, employees' continuous professional development, user education, and research and development initiatives;
- there is enforcement of cyber-security policy;

- there is compliance with pertinent legislation, regulations and policies.
- there are collaborations amongst interested parties within and external to the organisation – collaborations provide platforms to share information on the protection of information infrastructures; and
- appropriate culture of cyber-security is implemented across the organisation.

5.5. DEMONSTRATION OF HOW THE INTEGRATED DEVELOPMENT CYBER-SECURITY THEORY WORKS

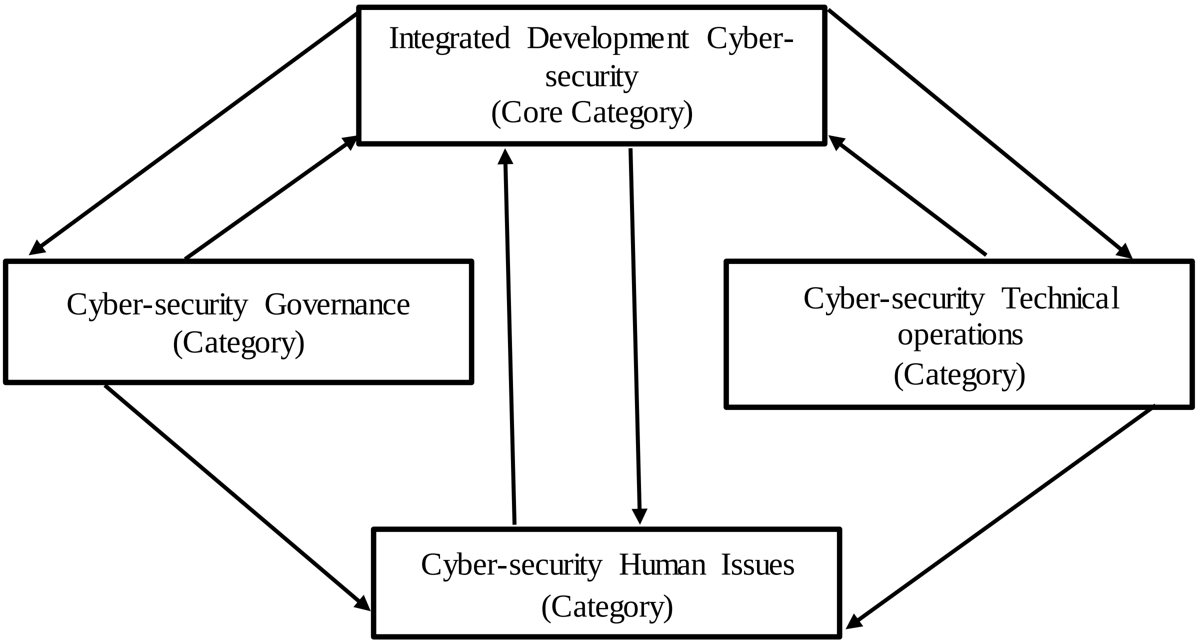

Integrated Development Cyber-security
(Core Category)
Cyber-security Governance
(Category)
Cyber-security Technical operations
(Category)
Cyber-security Human Issues
(Category)

Figure 5.2: Categories of the integrated development cyber-security theory

The participants indicated that the integrated development cyber-security is the glue holding together all the puzzles for successful implementation of the cyber-security programme in the metropolitan municipality. The integrated development core category is the structure that is responsible for inculcating the culture of cyber-security throughout the municipality. This structure ensures that an all-encompassing cyber-security policy is developed. Integrated development cyber-security ensures that there is an inventory of critical information infrastructure, and that the developed cyber-security policy covers all critical information infrastructures. The integrated development structure advises executive management on the industry best practices for cyber-security, and information infrastructure. After developing the cyber-security policy, the integrated development cyber-security custodian submits the policy to the cyber-security governance structure for official sign-off and to make the policy an official municipal document. To implement the cyber-security policy, the integrated development cyber-security structure formulates the cyber-security strategy that is aligned to the municipal IDP strategy. The strategy is also submitted to the cyber-security governance structure for approval, and to commit resources to achieve the strategy.

The cyber-security governance category mainly sets the right tone at the top because the role players in this category are the executive management who are driving the implementation of the municipal IDP. The cyber-security governance domain ensures that cyber-security is in the strategic risk management agenda. Cyber-security affects municipal business continuity which is a strategic priority. Cyber-security governance ensures that there are adequate resources to drive the implementation of the cyber-security programme by the integrated development cyber-security structure. Aligning cyber-security to the municipal IDP elevates the cyber-security agenda in the municipality, and therefore the buy-in from executive management in order to commit resources for cyber-security activities. Amongst other important roles of the cyber-security domain, is setting up the oversight structures that can hold management at all levels accountable for the control deficiencies in cyber-security and the information infrastructure environment. The cyber-security governance domain sets the cyber-security culture through the resources that drive the agenda of the information infrastructure protection against cyber-security threats.

The functions of the cyber-security technical operations domain take place in the various business units that are operating or working on information infrastructures. This category aligns the duties of pertinent employees to the cyber-security policy. The business units buy the information infrastructures with the intention of achieving their business objectives. The technical functioning of the controls implemented to secure the information infrastructure takes place in this domain. For example, the Finance unit implements a revenue management system to collect revenue from customers such as rate payers, and other municipal services that are paid for by the citizens. Access control to the revenue systems is implemented by the integrated development cyber-security domain, but monitored by the Finance unit. It is the cyber-security technical operations domain that determines if the cyber-security controls that have been implemented are assisting the business unit to achieve the business objectives. It is this domain that determines the risk appetite when it comes to information infrastructure protection. Cyber-security risk appetite determines how the integrated development cyber-security should drive the cyber-security programme for various information infrastructures. The business units employ people to use the information infrastructure in pursuit of business objectives. Technology can be implemented, but without people to operate it, it will not achieve the intended objectives. People who are employed within the business there are the first line of defence for securing the information infrastructures. Employees' knowledge, behaviour, and attitudes play an essential role in securing the information infrastructure against cyber-security threats. Business units employ people with minimum requirements to perform their duties while operating the information infrastructures. Due to the pace of changes in the cyber-security environment, and the information infrastructure environment, employees need to constantly keep pace with the innovation in these areas. Therefore, in order to address employees' issues in dealing with cyber-security, the human issues in the cyber-security domain are regarded as key issues.

The human issues in the cyber-security category involve individual employees that operate the information infrastructure in the municipality. The cyber-security governance domain sets the legislative and regulatory framework that includes, amongst others, the Labour Relations Act. The Municipal Systems Act requires the municipality to implement performance management systems. There is varied legislation that regulates how employees must be engaged and treated in the municipality. Within the ambits of the regulatory framework, human issues in the cyber-security category relate to ensuring that users are trained to work on the information infrastructure so as to minimise opportunity to commit errors when conducting their duties. This category ensures that employees/users, through the cyber-security awareness programme, are continuously made aware of the current trends of cyber-security threats and their impact on the information infrastructures that employees/users operate. The integrated development cyber-security domain drives the implementation of these cyber-security trainings and awareness programmes. It is for this reason that the integrated development cyber-security core category is the main driver to successfully implement cyber-security in the municipality. The integrated development cyber-security structure implements, facilitates, and co-ordinates the activities of the cyber-security programme.

5.6. INTEGRATED DEVELOPMENT CYBER-SECURITY THEORY (IDCT) EVALUATION

In conducting this study, the research was guided by Charmaz’s (2006) four criteria for credibility, originality, resonance, and usefulness in developing this substantive theory. The four criteria assisted the researcher to address the implicit actions and meanings in the phenomenon investigated and helped to analyse how it was constructed (Charmaz, 2006). The researcher sought to answer the four criteria’s associated questions in the affirmative way in order to comply with the GT evaluation guidelines.

Table 5.2: IDCT evaluation

	Criteria One - Credibility	**Response**
1.	“Has your research achieved intimate familiarity with the setting or topic?”	Yes
2.	“Are the data sufficient to merit your claims? Consider the range, number, and depth of observations contained in the data.”	Yes
3.	“Have you made systematic comparisons between observations and between categories?”	Yes
4.	“Do the categories cover a wide range of empirical observations?”	Yes
5.	“Are there strong logical links between the gathered data and your argument and analysis?”	Yes
6.	“Has your research provided enough evidence for your claims to allow the reader to form an independent assessment - and agree with your claims?”	Yes
	Criteria Two – Originality	**Response**
1.	“Are your categories fresh? Do they offer new insights?”	Yes
2.	“Does your analysis provide a new conceptual rendering of the data?”	Yes
3.	What is the social and theoretical significance of this work?	Yes ***
4.	How does your grounded theory challenge, extend, or refine current ideas, concepts, and practices?”	Yes ***
***** refers to the research conclusion, under research contribution section**		
	Criteria Three – Resonance	**Response**
1.	“Do the categories portray the fullness of the studied experience?”	Yes
2.	“Have you revealed both liminal and unstable taken-for-granted meanings?”	Yes

3.	“Have you drawn links between larger ‘collectivities’ or institutions and individual lives, when the data so indicate?”	Yes
4.	“Does your grounded theory make sense to your participants or people who share their circumstances? Does your analysis offer them deeper insights about their lives and worlds?”	Yes
	Criteria Four – Usefulness	
1.	“Does your analysis offer interpretations that people can use in their everyday worlds?	Yes
2.	Do your analytic categories suggest any generic processes? If so, have you examined these generic processes for tacit implications?	Yes
3.	Can the analysis spark further research in other substantive areas?	Yes
4.	How does your work contribute to knowledge? How does it contribute to making a better world?”	Yes ***
***** refers to the research conclusion, under research contribution section**		

5.7. CHAPTER SUMMARY

The ConGTM revealed the latent patterns of practitioners’ behaviour when dealing with cyber-security challenges in the municipality. One of the objectives of adopting the ConGTM was to discover a vigorous empirically resultant core variable or hypothesis. The resultant theory has earned its way through its undoubted demonstration that it represents the research participants’ main concern. Through the integrated set of hypotheses by the participants and the researcher, the theory was developed. The researcher applied his theoretical sensitivity to advance the objectives of the study and the study methods. Through the theoretical sampling, the researcher sampled the data until the participants’ main concern was discovered in the data being analysed. Within the chosen research population, the researcher sampled the participants’ input while busy collecting the data, hence it was not possible prior to conducting the research to state exactly what data would be required. The emerged core variable was derived at a point where the researcher reached a situation where no more new patterns surfaced from the data being collected, and at this point the data was considered to be saturated

Memoing was an important instrument for the researcher in deriving a substantive theory of integrated development cyber-security. The activities of memoing entailed writing up of ideas on the formulated codes as they were conceived by the researcher while conducting data coding in pursuit of data analysis. The researcher adopted memoing as a rationale to ideation and abstraction. At the beginning of the data analysis, memoing started out as short sentences but moved to be several pages long. Through constant comparisons of memos, and linking of various codes, theoretical coding was achieved. In theoretical coding there was both intuition and intellect on the side of the researcher in order to move from low level description to high level abstraction.

CHAPTER 6
MUNICIPAL CYBER-SECURITY FRAMEWORK

6.1. CHAPTER INTRODUCTION

Metropolitan municipalities require a framework to assess their cyber-security posture with the intention of enhancing the information infrastructure protection against cyber-risks. The researcher developed the framework from the substantive theory that was established through the ConGTM study. The framework served as the foundation to assess cyber-security status in the metropolitan municipalities in South Africa. The independent construct and the three independent constructs of the substantive theory were used as a basis to formulate the municipal cyber-security framework. Successful attainment of these three independent constructs guaranteed the *Integrated development cyber-security* which the research identified as a yardstick or benchmark against which to assess the cyber-security status in the metropolitan municipality environment.

Table 6.1: Independent constructs

Domain		**Processes**
Dependent variable/core category: Integrated development cyber-security		
1.	**Integrated development cyber-security**	Strategy development
		Policy development
		Organisation of cyber-security efforts
		Research and development
		Cyber-security steering committee
Independent construct 1: Cyber-security governance		
2.	**Cyber-security governance**	Risk management (Strategic risk register)
		Cyber-security sponsorship
		Cyber-security assurance
		Oversight committees
		IT governance
		Corporate governance best practices (King IV report)

Independent construct 2: Cyber-security technical operations		
3.	**Cyber-security technical operations**	Cyber-security tools & technologies
		Information infrastructure certifications
		Cyber-security monitoring & evaluation
		International standards & best practices
		Cyber-security policy enforcement
		Catalogue of critical information infrastructure
		Information infrastructure asset management
		Contingency planning & procedures
		Independent auditing of systems & methodologies
		Allocation of resources
		Operational risk management
		Programme performance management
Independent construct 3: Human issues in cyber-security		
4.	**Human issues in cyber-security**	Education & training
		User awareness
		Cyber-security policy enforcement
		Occupational certifications
		Affiliations to professional institutes
		Individual performance assessment
		Ethical conduct

6.2. DEFINING THE CYBER-SECURITY FRAMEWORK PROCESSES

6.2.1. Integrated development cyber-security

A. **Strategy development** relates to the development of a municipal-wide cyber-security strategy, allocation of implementation structures across municipal sectors, and an understanding of municipal cyber-security risks and threats which drive competencies at municipal-wide level. Cyber-security strategy is vital to uplift the cyber-security agenda across the municipality. A well-articulated cyber-security strategy helps prioritise cyber-security as an important policy area. This plan presents an organisational-wide vision and stance on cyber-security. It is important to align the cyber-security strategy to the organisation’s strategic objectives so that the allocation of resources will be directed towards achieving the organisation's objectives. A strategy is an all-encompassing plan as it includes all the municipal functional areas. Cyber-security strategy links the cyber-security programme to the municipal IDP. The allocation of funds to the cyber-security programme is recorded in the service delivery budget implementation plan (SDBIP).

B. **Policy development** entails developing a municipal-wide cyber-security policy, which ensures attainment of cyber-security strategy objectives. The cyber-security policy details the information infrastructure being referred to and what is meant by securing such an information infrastructure. Further, the cyber-security policy specifies the role players involved in securing the information infrastructure. If properly articulated, the cyber-security policy amongst other things, explicitly specifies what information infrastructures need to be protected and against what threats. The cyber-security policy also provides guidelines on the roles and responsibilities in implementing the cyber-security strategy.

C. **Organisation of cyber-security efforts** relates to the formation and maintenance of an overarching programme for cyber-security coordination, including authority (executive management), with a consolidated budget.

D. **Research and development** entails continuous exploration of how best to safeguard information infrastructure against cyber-threats. Research and development is driven by the three domains of governance, technical operations and human issues. This sustains the benefits derived from the adoption of cyberspace as a tool to achieve municipal objectives.

E. **Cyber-security steering committee** is a technical competent body that has no executive authority but advises management on the current trends, best practices, and emerging risks in cyber-security. This committee analyses cyber-security operational plans and measures implementation progress against the approved plans. This committee reports to executive management.

6.2.2. Domain 1: Cyber-security governance

A. **Risk management**, in the context of this study, is a process of identifying events or circumstances that can impact the municipality objectives. At a strategic level, risk management entails identifying those events or circumstances that influence the attainment of the organisation's strategic objectives. The influence could be positive or negative. A positive influence is one that enhances the opportunities to achieve the organisational strategic objectives. A negative influence is one that has a devastating or disastrous impact on the achievement of the organisation's strategic objectives. At a strategic level, the executive management team is responsible for identifying those events or circumstances that have a devastating impact on the achieving of strategic objectives. These negative events or circumstances are recorded in a strategic risk register wherein the mitigating controls to minimise the impact or likelihood thereof are also provided. The mitigating controls require management to commit resources and hence the involvement of the executive management team is essential. Cyber-related risks warrant the attention of the executive management team due to the potential impact they have on the delivery of municipal services.

B. **Cyber-security sponsorship** refers to financial commitment by executive management to fund the cyber-security programme in pursuit of the cyber-security strategy. Sponsorship is not a responsibility of one business unit, but a collective executive management team effort. If treated properly, cyber-security sponsorship sets the management tone and inculcates the culture of cyber-security across the organisation. Sponsorship addresses cyber-security at departmental (group) level, and at individual level through funding the education, training, and user awareness campaigns. Cyber-security impacts almost every business unit in the municipality, and therefore sponsorship cannot be the responsibility of only one individual business unit. The interconnectedness of information infrastructures warrants that every business unit that forms part of the interconnectedness must be part of the cyber-security sponsorship. Sponsorship can also be translated to a situation where executive management permits staff members to leave their work stations to attend to education and training, and other skills enhancement initiatives. By providing sponsorship to cyber-security, executive management is leading from the front and is providing necessary leadership for everyone else in the organisation to follow.

C. **Cyber-security assurance** entails providing an independent guarantee that the controls that management has implemented are working as intended to achieve the organisational goals. Risks present the possibility of not achieving the organisation objectives. The risks associated with cyber-security are enormous and could have devastating consequences should they materialise. Cyber-security risks are highly likely to happen and the possible impact includes non-delivery of municipal services.

Cyber-security assurance is a legislative requirement (MFMA) which requires the internal audit function to develop a risk-based internal audit plan in order to provide assurance on the controls implemented in the highest risk areas. Cyber risks are highest risk areas in the municipality as they affect the core mandate of the institution to deliver services to the local community. Industry best practice such as King IV report on corporate governance requires executive management to establish an internal audit committee to manage the activities of the internal audit function. The audit committee advises the municipal council on the internal controls, risk management, and governance processes that executive management has implemented to achieve organisational objectives. The office of the Auditor General of South Africa also performs assurance activities in the municipality. Cyber-security assurance presents an opportunity to identify weakness in the system of internal controls. It also presents an opportunity for consequent management to cyber-security delinquent employees. If properly implemented, cyber-security assurance strengthens the protection of the information infrastructure. Cyber-security assurance is the guardian of cyber-security governance processes.

D. **Oversight committees** are the governance structures within the municipality that strengthen accountability through monitoring and evaluation. Examples include the infrastructure portfolio committee, audit committee, and Exco. Oversight committees hold management accountable for non-delivery of municipal services, non-performance of performance targets, and non-compliance with applicable policies, legislation, and regulations.

E. **IT governance** refers to executive management's processes that delineate how the organisation directs and controls technology use and information infrastructure protection. IT governance is a component of corporate governance in the municipality. The ultimate aim of IT governance is to ensure that information technology continuously supports key business processes in order to sustain and enhance opportunities for meeting organisational objectives. IT governance promotes the implementation of cyber-security. Further, IT governance enhances information confidentiality, integrity and availability which are the core objectives for cyber-security.

F. **Corporate governance** is defined to mean setting and steering strategic direction of the organisation through ensuring accountability, development of policies, and providing oversight in the implementation of organisational strategy. Corporate governance also involves setting appropriate structures to ensure that the organisation achieves the set organisational objectives. Corporate governance processes ensure that governance processes take place and that the organisation is steered towards achieving business goals. Corporate governance processes include risk management, cyber-security governance, compliance with legislation, and regulations and reporting requirements. As part of corporate governance, the audit committee reports to municipal council on the effectiveness of controls that management has implemented to meet the organisational mandate and objectives.

6.2.3. Domain 2: Cyber-security technical operations

A. **Cyber-security programme management** refers to the composition and organisational design of cyber-security. This includes reporting structures, roles and responsibilities assigned to safeguarding the information infrastructure. Programme management plays a central role in implementing cyber-security policy. The cyber-security officer/chief information security officer is responsible to ensure that the tools and technologies utilised to safeguard information infrastructures are providing the security as defined in the cyber-security policy. Programme management provides formal structures with allocated cyber-security roles which aid in providing centralised coordination and facilitation of cyber-security activities in the organisation. This is the structure that ensures that cyber-security matters form part of the executive management agenda on corporate governance.

B. **Cyber-security tools and technologies** refer to the actual deployment of technologies and methodologies that are intended to provide information infrastructure protection. These technologies include anti-virus software, network monitoring tools, intrusion detection software, intrusion prevention tools, logging of users' and administrators' activities, and access control mechanisms. Access controls include both logical and physical access to information infrastructure assets. Logical access incorporates authentication processes where a user provides their user name and the corresponding password in order to gain access to the information technology system. Controlling physical access entails implementing security personnel and user identification tools in order to allow physical access to the information infrastructure assets. The deployment of security tools and technologies work hand in hand with industry best practices. The utilisation of tools and technologies aims to achieve the requirements of the cyber-security policy in pursuit of achieving the cyber-security strategy to support the attainment of business strategy objectives. Cyber-security tools and technology permit the availability of critical information infrastructures 24/7.

C. **Information infrastructure certification** entails meeting international and or national standards related to a specific information infrastructure. It also involves meeting the regulatory requirements specific to an information infrastructure. For example, the .zadna in the country, under the guardianship of the Department of Telecommunications and Postal Services manages the .za domain name space through issuing licences in terms of the Electronic Communications and Transactions Act (RSA, 2002). Another example is the ICASA which issues electronic communications operators and service providers licences according to the provisions of the Independent Communications Authority of South Africa Act of 2006 (RSA, 2006). The South African Bureau of Standards, through South African National Standards, plays an essential role in providing certifications – particularly those relating to process control systems.

D. **Cyber-security monitoring and evaluation** refers to systems that have been implemented to ascertain that the tools and technologies deployed to safeguard information infrastructures continue to provide the services expected. To achieve monitoring function, there are reports generated by various tools to give statistics in various areas. Statistics generated include information such as failed login attempts, illicit sites visited by employees, transaction history, audit trails, and trends in the network activities. The evaluation part deals with assessing the adequacy of the deployed technologies and methodologies in protecting the information infrastructure. Monitoring and evaluation ensures that cyber-security mechanisms are operated within the prescripts of relevant policies, legislation and regulations. Continuous monitoring and assessment inculcate and cultivate the culture of cyber-security as it enhances the protection of information infrastructures on an ongoing practice.

E. **International standards and industry best practices** involve accredited institutions that provide guidelines on the implementation of information infrastructures protection practices. The accredited institutions include ISACA for Cobit (IT governance framework), International Standards Organisation (ISO) for ISO/IEC 27000 suite, NIST, etc. Best practices are adopted to aid the institution to implement and monitor cyber-security. The standards aid to mitigate cyber-security risks. By adopting best practices, support received from vendors and service providers is enhances, as both the organisation and vendors have adopted the same practices which are transparent to pertinent stakeholders. Adoption of industry best practices minimises or limits dependence on individual heroism and insulated mechanisms which are difficult to manage, maintain, and recover in case of emergencies.

F. **Cyber-security policy enforcement** refers to the processes that management follows to ascertain that cyber-security policy is adhered to. After monitoring and evaluation exercises, gaps and weaknesses are identified. In situations where automating the processes for the protection of information infrastructure is an option, this is the preferred option because of consistency in application/functionality compared to manual processes of the same activity. For example, failed log in attempts of four or more should automatically disable the user profile. Also, visiting illicit websites should be automated and blocked. Users wanting to e-mail big amounts of data should be blocked or requesting permission from the system administrator. Unattended workstations, or where a session has been opened and no activity has taken place for five minutes (depending on the policy), the desktop should lock itself. When the user wants to continue using the system, the user must re-enter the credentials in order to get access. Information infrastructure must require users to change to change passwords after 30 days. All these activities are enforcement mechanisms that promote information infrastructure protection.

G. **Catalogue of critical information infrastructure** is a list of all critical information infrastructures in the municipality. The information infrastructures become critical information infrastructures if other infrastructures are dependent on them to deliver essential or critical services. Process control systems depend on ICT in order to operate as intended. PCS support the municipality's delivery of essential services such as electricity and clean water. Therefore, the information infrastructures that support the PCS that in turn support the delivery of essential services, are called critical information infrastructures. Management in the organisation must ensure that the organisation has a list of all municipal critical information infrastructures. The catalogue will assist management to put appropriate controls in place for such infrastructures. Cyber-security priority is guided by the available list of critical information infrastructures. Critical information infrastructures in the eThekwini

Municipality include computer networks, servers, software, computer applications, technologies and hardware. All of these support the critical infrastructures in the municipality of which incapacitation or destruction shall have a devastating influence on municipal well-being, security, economy, public health and safety.

H. **Information infrastructure asset management** relates to the identification of these assets and keeping an inventory thereof. Maintaining the asset inventory assists management to make informed decisions on information infrastructure acquisition or procurement, maintenance, and asset disposal mechanisms. Asset management assists in monitoring and managing software licences across the organisation. Contingency planning is linked to asset management because some information infrastructure assets are dependent on the vendors and service providers (consultants) for emergency support. 24/7 availability of critical information infrastructures is largely dependent on asset management processes. Information infrastructure asset management is also linked to the cyber-security helpdesk or service desk. The helpdesk logs all the service requests for specific assets which then creates a database of all problems and possible solutions to those problems in relation to a specific asset type, make, etc. Asset management facilitates speedy resolution of problems through the linkage with the service desk.

I. **Contingency planning and procedures** relate to proactively preparing for the unforeseen eventualities that have the potential of disrupting the normal functioning/operational effectiveness of the information infrastructure. Sometimes a contingency plan is known as plan B. If the normal information infrastructure processes are unexpectedly disrupted, what processes and procedures are in place to ascertain that those eventualities have minimum impact on the delivery of essential services? Properly planned disaster recovery plans and related procedures are examples of contingency plans. Contingency planning is a visionary method developed through suitable assessments aimed at dealing with the disruptions or adversaries on information infrastructure. This planning considers amongst other things the alternative approaches of operating the information infrastructures in case of disruption by using, for example, alternative practices which could incorporate alternate sites for operations and systems backup.

J. **Independent auditing on information infrastructures** entails assessing the controls design, and operational effectiveness of the controls that are implemented to achieve or meet the requirements of the cyber-security policy in pursuit of the cyber-security strategy and in turn the organisational strategy. This assessment is conducted by an independent function outside the assessed operational area. Independent assessments are conducted by the internal audit function, and the office of the Auditor General. Independent auditing is an indirect method to enforce compliance with cyber-security policies, legislation, and regulations. The aim of independent assessment of controls is to identify the weakness, if any, with the sole objective of strengthening the protection of information infrastructures in order to continue supporting the objectives and vision of the municipality.

K. **Operational risk management** involves pre-empting possibilities that could adversely affect the technical operations of cyber-security. Identified eventualities are assessed by the line function/management in terms of impact and likelihood. Operational risk management results in an operational risk register. It entails the identification of the threat, followed by the assessment of the risk (impact and likelihood), analysing the risk control measures, and implementing the risk control measures. A plan is formulated to implement the controls that have been chosen, which include time, resources and personnel needed to implement these control measures. The results of analysing the risk control measures include accepting the risk, avoiding the risk, controlling the risk, and transferring the risk. Cyber-security operational risks include threats from a virus, worms, denial of service attacks, natural disasters, hackers, non-compliance, etc.

L. **Allocation of resources** involves scheduling and assigning resources according to the operational requirements to operate a particular information infrastructure. Some information infrastructures require 24/7 availability. Personnel are required to ensure that 24/7 availability is attained and hence the scheduling of resources to achieve this requirement. Personnel may be required to work overtime, hence the criticality of allocating relevant resources including financial resources. Poor allocation of resources could result in unattended emergency situations with devastating consequences in the service delivery mandate of the municipality. Physical security of the information infrastructure also depends on the allocation of pertinent resources to achieve the required level of protection. Allocation of resources must be commensurate with the criticality of the information infrastructure.

M. **Programme performance management** involves setting targets and operational plans against which to measure performance. Achieving optimum security requires setting of targets and actions plans needed to achieve the same. Performance management entails assessing the programme performance against the set cyber-security objectives. Performance management in the municipality environment is a legislative requirement, and has to be audited by an internal audit and the office of the Auditor General. Assessing programme performance management is a tool to identify areas that need improvement to achieve optimum protection of information infrastructures against cyber-risks. Therefore, programme performance management aims to attain effectiveness and efficiency in the provision of cyber-security across the organisation.

6.2.4. Domain 3: Human issues in cyber-security

A. **Education and training** relates to providing employees and consultants with the required skills and knowledge in relation to cyber-security policies and procedures as applicable to their job requirements. Employees can receive training through on-boarding induction, and through continuous on-the-job training. Training can be in the form of formal education where employees are trained to obtain an educational qualification or professional certification. Training can also be informal, for example through attending seminars, conferences, breakfast sessions, etc. There are no formal examinations for informal training. Education and training in cyber-security ensures that employees have the right qualification and skills mix to perform their duties in pursuit of information infrastructure protection against cyber-threats. The first line of defence against cyber-attacks is a well-trained staff.

B. **Cyber-security user awareness** relates to sensitising users of information infrastructures to the cyber-risks. It is essential to establish and maintain a cyber-security awareness programme that is robust to ensure that information infrastructure users are alert and responsive to the importance of guarding sensitive information and related infrastructure against the cyber-risks. The institution can invest heavily in technical automated controls to protect information infrastructures; however, these technical controls can be rendered useless when staff lack cyber-security awareness. Cyber-security awareness assists in the reduction of cyber-security breaches and related possibilities by providing well-intentioned staff with the knowledge to avoid becoming inadvertent attack vectors, for instance such as by unintentionally downloading malware.

C. **Cyber-security policy enforcement** includes making users of the Internet and e-mail systems to sign acknowledgement and understanding of the acceptable usage of these applications. Further, it is to make users aware that their activities on information infrastructure are monitored by management. If users are aware that their actions are monitored, they conduct themselves and their activities in an acceptable way. Cyber-security policy violations and breaches are properly reported to relevant structures and investigated as directed by the policies. Disciplinary processes are instituted to those found to have performed illicit activities on information infrastructures.

D. **Occupational certifications** relate to writing a profession-related board examination in order to obtain occupation specific certification and or designation. For example, those personnel who work on the telecommunications network need to write examinations for a certified network engineer/professional designations. Those that specialise in information security need to write a board examination to become certified in information security and or cyber-security. Some network vulnerability assessment tools require specific qualifications in order to be able to utilise the tool. To conduct an audit on the information technology environment requires a certified information systems auditor designation. Occupational designations give comfort to management and other stakeholders that personnel have what it takes to protect information infrastructures against cyber-threats. Affiliation to professional institutes is a pre-requisite for writing board examinations.

E. **Affiliation to professional institutes** relates to joining occupational institutes or organisations that promote specific occupations. For example, internal auditors join or become members of the Institute of Internal Auditors (IIA) which is the body that prescribes standards and principles to be followed when conducting an internal audit function. Generally, professional institutes are credible organisations that provide guidelines to be adopted by affiliated members. Professional institutes offer a body of knowledge where affiliates come together and share their experiences and possible solutions to challenges encountered by members when conducting their job responsibilities. Professional institutes have prescribed minimum ethical standards that all members needs to abide by. Membership can be revoked by the institute if the prescribed minimum standards and ethical behaviour requirements are breached or compromised (bringing the profession into disrepute). Professional institutes convene and hold regional/national conferences where topical issues affecting the profession are discussed by the industry experts and other key stakeholders. Some affiliations require members to meet the minimum requirements annually in order to keep their membership active. They require continuous professional development (CPD) to take place in a financial year/annually. These CPD requirements promote the members to be on par with the current trends affecting the profession.

F. **Individual performance assessment** relates to setting employee-based performance targets driven by the job description of the employee. Assessing individual performance aids in determining the competency of an employee in achieving the requirements of the job occupied. Each employee signs a performance contract against which performance will be assessed. The intention of performance assessment is to determine if there are any areas in which an employee needs assistance to achieve the requirements of the job. If gaps have been identified, the supervisor and the employee concerned formulate an improvement plan which entails a personal performance improvement plan. Training and supervision are some of the activities that can be included in the personal performance improvement plan. In the cyber-security context, individual performance assessment aims to strengthen the protection of information infrastructures. If employees are assessed and found to be competent, they are rewarded and encouraged to maintain and enhance their performance.

G. **Ethical conduct and behaviour** entail prescribing moral standards that clearly distinguish acceptable behaviour from unacceptable behaviour. The information infrastructure environment is a sensitive area where employees are expected at all times to demonstrate a high level of trustworthiness, and conduct themselves in a manner that will not compromise the protection of information infrastructures. For example employees are not allowed to divulge organisational sensitive information to the public or anyone else who is not supposed to have knowledge of such information. Depending on the criticality of the information infrastructure, security clearance is required from the state security agencies.

6.3. PROPOSED MUNICIPAL CYBER-SECURITY FRAMEWORK

The proposed cyber-security framework can be adopted by the metropolitan municipalities as a starting point to secure their information infrastructure against cyber-security threats.

This framework forms the basis for cyber-security controls to be implemented to secure the infrastructure against cyber threats.

Table 6.2: Proposed municipal cyber-security framework

METROPOLITAN MUNICIPALITY (ORGANISATION)
INTEGRATED DEVELOPMENT CYBER-SECURITY (Key Role players - Cyber-security Specialists)
Cyber-security Policy Development
Cyber-security Strategy Development
Centralised Cyber-security Coordination
Cyber-security Research & Development
Cyber-security Steering Committee
Alignment with IDP

PILLAR A	PILLAR B	PILLAR C
CYBER-SECURITY GOVERNANCE (Key Role players – Management level)	**CYBER-SECURITY TECHNICAL OPERATIONS** (Key Role players – Business Units level)	**HUMAN ISSUES IN CYBER-SECURITY** (Key Role players – employees level)
Risk Management	Cyber-security Programme Management	Education and Training
Cyber-security Sponsorship	Cyber-security tools and technologies	Cyber-security awareness
Cyber-security Assurance	Information Infrastructure Catalogues	Policy enforcement
Oversight Committees	Information Infrastructure Asset Management	Occupational certifications
IT Governance	Cyber-security monitoring and evaluation	Affiliation to professional institutes
Corporate governance	International standards and best practices	Individual performance assessment
Legislative Framework	Programme Performance Management	Ethical conduct and behaviour
	Cyber-security policy enforcement	
	Contingency planning and procedures	
	Cyber-security Auditing and Assurance	
	Cyber-security Resource allocation	

6.4. APPLYING THE MUNICIPAL CYBER-SECURITY FRAMEWORK

Metropolitan municipalities exist to deliver basic services to the citizens as stipulated in the Municipal Systems Act. A centralised cyber-security portfolio is the foundation for successful implementation of the municipal cyber-security framework. Centralised cyber-security is responsible for facilitating the creation of information infrastructure inventory across the organisation. An inventory of information infrastructure assists to identify various information infrastructure assets and their respective properties. A comprehensive information infrastructure catalogue guides the development of cyber-security policy. This policy covers all business units in which information infrastructure assets exist. The policy provides guidance on the expected safeguarding methods, tools, techniques, and mechanisms to be adopted to implement minimum information infrastructure safeguarding. Cyber-security policy must be approved at the highest level within the municipality in order to be effective.

Cyber-security policy informs the development of cyber-security strategy, which must be annually approved at the right level of authority. The cyber-security strategy covers information infrastructure assets across the municipality and requires buy-in from the heads of the business units. The cyber-security strategy must be aligned to the municipal-wide business strategy which is the integrated development plan. This alignment can be achieved through the integrated approach to cyber-security. The integrated approach to cyber-security implementation strategy guides the allocation of a consolidated budget towards cyber-security enactment. The cyber-security budget will be aligned to or be commensurate with the SDBIP as guided by the requirements of the MFMA. The centralised approach to cyber-security implementation enhances research and development on cyber-security, and effective collaboration amongst the pertinent stakeholders at various levels within the municipality and across various spheres of governments in the country. A centralised approach to implement cyber-security encourages the formulation of a cyber-security steering committee whose intention amongst others is to drive the technical monitoring of the cyber-security strategy implementation.

Executive management's buy-in of the successful implementation of cyber-security in the municipality is essential. Their buy-in inculcates the culture of cyber-security and sets the right tone at the top to safeguard information infrastructure assets. As part of showing their buy-in, executive authority must approve the cyber-security policy, and related cyber-security implementation strategy. Management's buy-in can be demonstrated through the appropriate allocation of an adequate budget in pursuit of cyber-security objectives. Also, it can be shown through various means such as setting of pertinent oversight structures, such as the audit committee and portfolio committees, to establish a necessary regulatory framework that is relevant to securing organisational information infrastructure assets, commissioning necessary reporting mechanisms, and elevating cyber-security risks to the strategic risk register since cyber-security weaknesses affect municipal business continuity and have cascading and devastating consequences.

Each business unit that operates an information infrastructure is responsible for deploying technologies and pertinent processes for cyber-security. Operating technologies and information technology require different processes and tools to safeguard their information infrastructure assets and hence respective business units driving their cyber-security implementation processes. The implementation of cyber-security processes must be guided by industry-specific best practices, and international and industry-specific standards.

The implementation of cyber-security policy must be aligned to human resources policies and related procedures such as recruitment policy, performance management policy, and employees' disciplinary policy. Employees are the first line of defence in cyber-security. Even if the appropriate technologies are implemented towards the protection of information infrastructure assets, they may not work or achieve the intended purpose if the human beings are not committed to securing such assets. Therefore, it is necessary that the centralised cyber-security implementation adopts a combined and comprehensive recognition of human issues in cyber-security. Human issues include processes such as cyber-security user awareness campaigns that are pertinent to the information infrastructure being operated. Cyber-security policy and other related policies must be communicated across the municipality. Proper communication of the relevant policies enhances situations to hold users accountable for their behaviour and actions regarding information infrastructures. Training and development of employees on cyber-security implementation is driven by the performance management processes of individual employees.

6.5. BENEFITS OF MUNICIPAL CYBER-SECURITY FRAMEWORK

A municipal cyber-security framework can provide guidelines to management in implementing the necessary information infrastructure safeguarding mechanisms across the organisation. The framework provides management with a holistic and comprehensive view of cyber-security components (categories). The municipal cyber-security framework assists management at various levels to understand who is influenced by a specific category and the possible impact. The framework is industry specific and is compatible with any legislation that is applicable to local governments in the country. Currently there is no known industry-specific cyber-security framework. Municipalities are guided by international standards and pertinent industry best practices which are necessary but not sufficient to address the unique cyber-security challenges of the metropolitan municipalities. In adopting the current approaches, municipalities are required to adapt and apply these practices, and the adaption process requires a considerable amount of time which is a catalyst for failure.

The municipal cyber-security framework will guide management in administering cyber-security implementation and to promote the acceptable cyber-security level that is necessary in establishing a desirable cyber-security culture and the subsequent maintenance thereof. The framework can be used to monitor and improve the controls that management have implemented to minimise or eliminate cyber-security threats. With minimal adaptation, the framework can be adopted as reference to understand the posture of cyber-security at any given point in time. The framework serves a basis for developing a cyber-security assessment instrument as it enables such a tool to conform to content validity. The framework provides a basis for defining the items to be assessed in order to determine the status of cyber-security in a municipality.

6.6. CHAPTER SUMMARY

The main purpose of this chapter was to present the municipal cyber-security framework developed in this study. The framework was developed from the ConGTM processes. The framework processes were defined in order to provide context for each category of the framework. Some processes overlapped amongst the categories; however, the intention of the framework is to guide the implementation of cyber-security controls to secure the information infrastructure against the cyber-security threats.

CHAPTER 7
AN INSTRUMENT TO ASSESS CYBER-SECURITY

7.1. CHAPTER INTRODUCTION

Based on the ConGTM study, a framework to implement cyber-security was developed. The researcher used the cyber-security framework to develop the assessment tool.

7.2. THE METROPOLITAN MUNICIPALITY CYBER-SECURITY ASSESSMENT TOOL

7.2.1. The design of the questionnaire

The statements for the questionnaire were developed from the cyber-security framework developed from ConGTM. The questionnaire was designed with the intention to be completed anonymously by the participants. The study employed a Likert-type scale structured questionnaire with closed-ended questions with five option answers to each question. The participants needed to choose the option that best described the situation of the question asked.

<table>
<tr><td colspan="5"><b>Metropolitan Municipality Cyber-security Assessment Survey Questionnaire</b></td></tr>
<tr><td colspan="5"><b>Legend:</b> SA = Strongly Agree, A = Agree, DK = Don’t Know, D = Disagree, SD = Strongly Disagree</td></tr>
<tr><td colspan="5"><b>INTEGRATED DEVELOPMENT CYBER-SECURITY DOMAIN</b></td></tr>
<tr><td></td><td><b>Please choose the statement that best describes your view</b></td><td colspan="3"></td></tr>
<tr><td></td><td></td><td><b>YES
1</b></td><td><b>NO
0</b></td><td><b>DON’T KNOW
2</b></td></tr>
<tr><td>1.</td><td>My organisation has a written cyber-security policy</td><td></td><td></td><td></td></tr>
<tr><td>2.</td><td>My organisation has an overarching supply chain management policy that guides the acquisition of information infrastructure</td><td></td><td></td><td></td></tr>
<tr><td>3.</td><td>My organisation has a documented cyber-security strategy</td><td></td><td></td><td></td></tr>
<tr><td>4.</td><td>My organisation has an inventory of critical information infrastructure</td><td></td><td></td><td></td></tr>
<tr><td>5.</td><td>My organisation has information infrastructures contingency plans</td><td></td><td></td><td></td></tr>
</table>

		SA 5	A 4	DK 3	D 2	SD 1
6.	The cyber-security policy is constantly reviewed to incorporate emerging trends in the protection of information infrastructures					
7.	The cyber-security policy contains sections that are relevant to my job					
8.	The cyber-security policy is aligned to the municipal Integrated Development Plan (IDP)					
9.	I believe our cyber-security strategy is aligned to the municipal IDP					
10.	There is a structure or unit within my organisation that is responsible to implement the cyber-security strategy					
11.	I know what to do if I want to report breaches or violations of the cyber-security policy					
12.	I know who the custodian of the cyber-security policy is					
13.	My organisation conducts research and development with the aim to enhance protection of the information infrastructure					
14.	Protection of the information infrastructure in my organisation is guided by the industry best practices					
CYBER-SECURITY GOVERNANCE DOMAIN						
		YES 1	**NO 0**	**DON'T KNOW 2**		
15.	My organisational strategic risk register contains cyber-security risk					
		SA 5	**A 4**	**DK 3**	**D 2**	**SD 1**
16.	Management has allocated adequate budget to implement a cyber-security policy					
17.	Risk management processes guide the implementation of cyber-security controls in my organisation					
18.	Management has provided guidance on the regulatory requirements pertaining to the information infrastructure that I work with					
19.	Management has allocated adequate people to protect the information infrastructures					
20.	Management enforces compliance to cyber-security					
21.	In my organisation there are oversight structures/committees that hold management to account for the protection of information infrastructure					

22.	Internal audit operational plans incorporate audits or reviews on information infrastructures on an annual basis					
23.	Management has input in the internal audit operational plan before the plan is implemented					
24.	Audit committee approves the internal audit operational plan before the plan is implemented					
25.	Management has implemented clear asset management practices					
26.	Management understands the possible impact of cyber-security threats to municipal service delivery					
CYBER-SECURITY TECHNICAL OPERATIONS DOMAIN						
		YES **1**	**NO** **0**	**DON'T KNOW** **2**		
27.	There are service level agreements between my municipality and the service providers working on information infrastructures					
		SA **5**	**A** **4**	**DK** **3**	**D** **2**	**SD** **1**
28.	Management is monitoring the services provided by the service providers/consultants against the service level agreements					
29.	My organisation has deployed technologies to protect information infrastructures against cyber-threats					
30.	Access to information infrastructures is controlled through identification and authentication					
31.	Management has adopted industry best practices to protect information infrastructure against cyber-threats					
32.	Anti-virus software is installed on our laptops, desktops, and other devices					
33.	Audits are conducted to provide assurance on the adequacy and effectiveness of controls that have been implemented to protect information infrastructure					
34.	The incident management procedures are adequate to resolve cyber-security incidents					
35.	The building that I work in is adequately protected to secure the information infrastructure					
MANAGE HUMAN ISSUES IN CYBER-SECURITY DOMAIN						
		SA **5**	**A** **4**	**DK** **3**	**D** **2**	**SD** **1**
36.	Employees' activities in information infrastructure are monitored					

37.	In my organisation, action is taken against employees who violate the cyber-security policy					
38.	Employees are made aware of the cyber-security policy contents					
39.	Employees know where to report suspicious illicit cyber-security activities					
40.	Employees receive adequate training in the information infrastructure they operate					
41.	I am aware of cyber-security threats affecting the information assets I work with					
42.	I am aware that organisational internet and e-mail systems should be used for business purposes					
43.	Employees accept responsibility for information infrastructure protection					
44.	My organisation constantly conducts cyber-security assessments to determine how employees are complying with the cyber-security policy					
BIOGRAPHICAL INFORMATION						
45.	I have been in the employ of the municipality for	• Less than 3 years = 1 • 3 years but less than 5 years = 2 • 5 years but less than 7 years = 3 • 7 years but less than 10 years = 4 • 10 years and over = 5				
46.	I belong to	• Information and Communication Technology Category = 1 • Operating Technology = 2 • Administration Category = 3				
47.	My position is at	• Management level = 1 • Specialist level = 2 • Clerical level = 3				

The statements in the assessment instrument are based on the cyber-security framework, specifically the processes that describe the four domains. All controls that are implemented to mitigate aspects of cyber-security must be evaluated to obtain assurance that they function the way they were intended to. The controls implemented include processes, procedures, technology and personnel. Assessments can be technical as well as non-technical.

7.3. RATIONALE BEHIND THE ASSESSMENT INSTRUMENT

The cyber-security instrument is as a result of the ConGTM where the research participants painted a picture of activities to be carried out in order to successfully implement the cyber-security programme in the metropolitan municipality. The researcher applied a theoretical sensitivity and memoing process during the data collection and analysis stage of the research to construct the rationale behind each statement in the assessment instrument.

Metropolitan Municipality Cyber-security Assessment	
INTEGRATED DEVELOPMENT CYBER-SECURITY DOMAIN	
1.	**My organisation has a written cyber-security policy** (a) Why cyber-security policy is necessary Cyber-security policy gives authority to the implementation of cyber-security in the municipality. This policy must be signed by the municipal council or delegated authority. The signed cyber-security policy signals the position of the municipal council on cyber-security. The signed cyber-security policy therefore becomes the benchmark against which to assess compliance with the protection of information assets from cyber threats. Cyber-security policy is a key socio-organisational resource that guides employees on how to ensure cyber-security when utilising information infrastructure assets while performing their duties. Cyber-security policy provides a baseline upon which to safeguard information infrastructure assets against cyber-related threats. (b) Risks associated with the lack of cyber-security policy Weakness in cyber-security could result in disturbance of the continuous provision of essential services, particularly those that whose delivery are dependent on the information infrastructure assets within the municipality. These essential services include delivery of water and electricity. Municipal administration processes could also be affected by the weakness in cyber-security due to the dependence on ICT. Cyber-security policy is one of the essential controls and is focused on the human domain in the protection of information infrastructure assets within the organisation. Lack of cyber-security policy could result in difficulty in measuring or assessing compliance with the organisational cyber-security position/expectation of cyber-security. Consequence management in the cases related to cyber-security breaches could be difficult to achieve. (c) Recommended practice for cyber-security policy The policy must be documented and approved by the highest authority in the municipality. It must contain all the cyber-security expectations on organisational information infrastructure assets. The policy must be updated continuously,

	preferably at least annually, and as dictated by the current trends in the cyber-security environment. Access to the cyber-security policy must be available to all employees. The owner of the cyber-security policy must ensure that users/employees are aware of the policy.
2.	**My organisation has an overarching supply chain management policy that guides the acquisition of information infrastructure** (a) Why supply chain management policy is necessary Control over the acquisition of information infrastructure assets is essential for addressing cyber-security concerns. Information infrastructure assets must be procured from only trusted and properly vetted vendors and service providers. Vendors and service providers become key stakeholders in ensuring business continuity. Cyber-security weakness could impact business continuity. Role players in business continuity are required to uphold ethical conduct and trustworthiness beyond reproach. Supply management policy is a control measure to ensure that the municipality conducts business with only credible vendors and services providers. (b) Risks associated with the lack of supply chain management policy Without trusted partners in business continuity, there is a possibility of disruption to service delivery. Information infrastructure assets could be procured to dodgy vendors and service providers, thereby compromising protection of information assets, and subsequently municipal business continuity. Procurement of information infrastructure assets could be difficult to control and monitor. There could be manipulation of the procurement process to inspire fraud and corruption which could result in dependency on service providers, poor quality of the procured materials, and other weaknesses which could result in compromising the cyber-security in the municipality. (c) Recommended practice for supply chain management policy All types of procurement must be guided by an approved supply chain management policy. The policy must stipulate guidelines for each type of the materials/services to be procured, including emergency procurements. The policy must provide guidelines on the conditions for service providers and vendors to comply with in order to be accepted and recorded in the municipal suppliers' database. An audit on the supply chain management policy incorporating the suppliers' database must be conducted at least annually by an independent assessor of internal controls. Supply chain management policy must prescribe minimum requirements for the acquisition of information infrastructure assets/services and contract management.
3.	**My organisation has a documented cyber-security strategy** (a) Why cyber-security strategy is important

	Cyber-security strategy elevates the cyber-security agenda across the municipality. Cyber-security strategy is the business case for cyber-security in the organisation as it presents and prioritises cyber-security as an important area, assigns roles and responsibilities, and highlights all forms of required commitment from all key stakeholders. Cyber-security strategy that is properly aligned to municipal strategy permits the allocation of resources on the areas of highest priority based on the risk assessment exercise. Cyber-security strategy provides the framework against which to measure the cyber-security implementation progress. (b) Risks associated with the lack of cyber-security strategy Lack of cyber-security strategy presents difficulty in monitoring and controlling the implementation of cyber-security. Allocation of resources relating to cyber-security measures could be skewed, not aligned to the municipal business strategy and might not be based on high priority areas. There could be a lack of co-ordination when implementing cyber-security measures in the municipality. Lack of co-ordination could lead to costly duplication of efforts and wastage of valuable resources. The budget to implement cyber-security initiatives resides in each business unit without a distinct cyber-security budget line item. (c) Recommended practice for cyber-security strategy The municipality must document and approve the cyber-security strategy. The strategy must be approved by the highest decision-making body in the municipality. The strategy must be aligned to the municipal business strategy which is the Integrated Development Plan (IDP). Progress on the implementation of cyber-security measures must be reported to the cyber-security committee or any equivalent or higher structure in the municipality. The cyber-security strategy must be reviewed at least annually. There must be continual reviewing and refinement of cyber-security strategy with the intention of adapting to changing a cyber-environment and threats landscape. There must be a single cyber-security strategy in the municipality that drives the cyber-security programme with a designated coordinating structure and mandate to drive cyber-security implementation across the organisation
4.	**My organisation has an inventory of critical information infrastructure** (a) Why an inventory of critical information infrastructure is important Identification, location, and functionality are amongst the essential record properties to be kept on each critical information infrastructure in the municipality. An inventory of critical information infrastructure facilitates ensures the safeguarding of such assets. Critical information infrastructures are convolutedly interdependent and interrelated. An appropriate inventory of information infrastructure assets ensures that all critical infrastructures that are reliant on critical information infrastructures are covered and are afforded the necessary cyber-security. Auditing and monitoring

	of controls implemented by management to safeguard such information assets become easier. Asset management processes, including procurement and maintenance also become easier, thereby ensuring business continuity. (b) Risks associated with the lack of critical information infrastructure inventory Lack of a critical information infrastructure inventory could lead to inadequate protection of such assets. Appropriate planning of the necessary safeguarding measures required to protect critical information assets could be compromised since some of such critical assets might not be covered due to deliberate or erroneous omission. Protection of all critical information infrastructures against cyber threats could not be ascertained. (c) Recommended practice for the critical information infrastructure inventory The municipality must formulate and maintain an inventory of critical information infrastructure assets. This inventory must be approved by the highest decision-making body within the municipality. There must be a designated structure within the municipality that is responsible for the compilation of a critical information infrastructure inventory. Access to the critical information infrastructure inventory must be controlled and only allowed to those that are permitted to have such access. There must be resources assigned to each critical information infrastructure asset for business continuity or emergency purposes.
5.	**My organisation has information infrastructure contingency plans** (a) Why information infrastructure contingency plans are important Information infrastructure contingency plans guide the testing and implementation of business continuity plans in case there is disruption to the normal functioning of information infrastructure. The plans provide procedures to be followed after disruption to normal business in order to restore normal functioning of such assets. Roles and responsibilities are clearly defined and the role players are engaged accordingly. Key stakeholders know what to do in the case of emergency or disruption to normal functioning of these assets (b) Risks associated with the lack of critical information infrastructure contingency plans There could be delays in the recovery process due to untested and uncoordinated recovery processes. There could be costly duplication of efforts. Cyber-security, particularly information security could be compromised. Disruption to the service delivery mandate could be prolonged which could result in loss of human lives and civil society protests/unrest. (c) Recommended practice for the critical information infrastructure contingency plans

	Critical information infrastructure contingency plans must be documented and regularly tested and signed off by the appropriate authority in the municipality. These contingency plans must be facilitated by a central designated structure with appropriate mandate and authority. Coordination of testing procedures must be centrally driven to ensure participation by all relevant key stakeholders.
6.	**The cyber-security policy is constantly reviewed to incorporate emerging trends in the protection of information infrastructures** (a) <u>Why constantly reviewing of cyber-security policy is important</u> Cyber-security policy must be relevant to the existing circumstances impacting information infrastructure. The policy must address current cyber threats. As technology evolves, so does the cyber-security policy. Adoption of technology requires security evolution that is commensurate with the pace of change in the technology environment. Reviewing of cyber-security policy must be aligned to the pace of the changes impacting the technology currently used by the municipality. To remain relevant, the cyber-security policy must be constantly reviewed and updated accordingly. (b) <u>Risks associated with the lack of cyber-security reviews</u> There could be non-alignment of the cyber-security policy to the current technologies that are utilised by the municipality. The policy might not fully/adequately address the safeguarding of information infrastructure assets. There could be misalignment of municipal expectations and the current practices on the ground, and subsequently this could lead to difficulty in holding people accountable in cases of cyber-security breaches. Consequence management could be difficult to implement. (c) <u>Recommended practice for continuous reviewing of cyber-security policy</u> Cyber-security policy must be continuously reviewed and the changes resulting from such reviews must be appropriately approved. The structure that is responsible for cyber-security policy must conduct such continuous reviews. Relevant stakeholders must be properly consulted during the review process in order to ensure completeness of the review process and buy-in from all key role players. Changes to cyber-security policy must be appropriately communicated across the organisation in order to enhance compliance with such policy.
7.	**The cyber-security policy contains sections that are relevant to my job** (a) <u>Why cyber-security policy must contain job-related sections</u> To be relevant, cyber-security policy must address job-related activities and management expectations from employees when performing their duties. Compliance with cyber-security policy must be aligned to individual performance assessment. Aligning cyber-security policy to employees' duties provides guidelines on the protection of information assets while performing their individual duties. The

	cyber-security policy assigns and confirms each employee's responsibility in the safeguarding of information infrastructure assets. (b) Risks associated with non-alignment of cyber-security to employees' duties Non-alignment could render cyber-security meaningless to the employees because they cannot relate to their duties. Management's expectations from employees on the protection of information infrastructure might not be appropriately communicated to relevant employees. If not aligned to individual duties, the cyber-security policy cannot be enforceable and compliance with it could be a challenge to achieve. Consequence management in cases of cyber-security breaches could be difficult to implement. (c) Recommended practice for aligning cyber-security policy to individual duties In order to be enforceable, the cyber-security policy must be aligned to the duties of each employee who is working on the information infrastructure assets. Each employee working on information infrastructure must on an annual basis sign acknowledgement of understanding the contents of the cyber-security policy that is applicable to their working environment.
8.	**The cyber-security policy is aligned to the Municipal Integrated Development Plan (IDP)** (a) Why aligning cyber-security policy to the municipal IDP is important Aligning cyber-security policy to the IDP gives authority to resource allocation in pursuit of information infrastructure protection. Buy-in from relevant key stakeholders could be accomplished as all forms of commitment are required from various stakeholders including top management. Attaching IDP to cyber-security initiatives could attract commitment and legitimacy of the whole cyber-security agenda across the municipality. (b) Risks associated with non-alignment of cyber-security policy to the municipal IDP Non-alignment to the IDP could render cyber-security policy a cosmetic exercise, and subsequently have no commitment and sponsorship from key stakeholders. Return on cyber-security investment could be difficult to ascertain. Allocation of cyber-security resources could be misdirected, thereby compromising the protection of information infrastructure assets. The basis for resources allocation could be difficult to substantiate, thereby distancing commitment to and sponsorship of cyber-security investment. (c) Recommended practice for aligning cyber-security policy to the municipal IDP Cyber-security policy must be aligned to the municipal IDP in order to attract commitment and sponsorship from management and other relevant stakeholders. When the municipal IDP has been reviewed, the cyber-security policy alignment

	must be re-visited in order to incorporate the changes, if any. Aligning cyber-security policy to IDP elevates the cyber-security agenda across the organisation. Breaches of cyber-security policy must be linked to the possible impact in order to determine the level of disciplinary action.
9.	**I believe our cyber-security strategy is aligned to the municipal IDP** (a) Why aligning cyber-security strategy to the municipal IDP is important The municipality is in the business of service delivery to the citizens. Therefore aligning the strategy to the IDP could enhance sponsorship opportunities. Everyone in the municipality performs to achieve the service delivery mandate of the municipality. Linking cyber-security initiatives to municipal service delivery enhances the elevation of the cyber-security agenda. An appropriately linked cyber-security strategy is a gateway to other spheres of government's involvement. (b) Risks associated with non-alignment of cyber-security strategy to the municipal IDP Non-alignment could lead to disregard of cyber-security initiatives, thereby compromising the protection of information infrastructure. There could be lack of commitment to and sponsorship of cyber-security initiatives. There could be inappropriately protected information infrastructure assets. Misalignment of cyber-security strategy could render the strategy meaningless which could lead to wasteful and fruitless expenditure. Allocation of resources could be difficult to substantiate. (c) Recommended practice for aligning cyber-security strategy to the municipal IDP Cyber-security strategy must be aligned to the municipal IDP in order to attract sponsorship and elevate the cyber-security agenda. After municipal IDP review, cyber-security strategy must be reviewed in order to ensure and enhance alignment. This alignment could enhance the safeguarding of information infrastructure because cyber-security initiatives will be commensurate with the essential services that ought to be provided, as outlined in the IDP document.
10.	**There is a structure or unit within my organisation that is responsible to implement the cyber-security strategy** (a) Why a designated cyber-security structure is important A designated cyber-security structure facilitates and coordinates the efforts to protect information infrastructure against cyber-related threats. Assigning cyber-security responsibilities to a designated structure enforces accountability towards cyber-security implementation initiatives. A designated structure could enhance research and development in the cyber-security environment in the municipality. Reporting on the progress of cyber-security implementation is centralised and enhanced. (b) Risks associated with disjointed implementation of cyber-security strategy

	There could be disjointed reporting, monitoring, and control of cyber-security activities. This disjointed situation could lead to inconclusive information for appropriate decision making on cybersecurity initiatives and investments. Appropriate metrics, data, monitoring processes and trends could be difficult to obtain and maintain to inform decision making to enhance the protection of information infrastructure assets. (c) Recommended practice for assigning a designated structure that is responsible to implement cyber-security strategy A designated cyber-security structure must be established. This structure has the responsibility to write and revise cyber-security policy and strategy. The designated structure will have the authority to implement and monitor progress against the cyber-security strategy. The designated structure is the first port of call when users/employees experience or want to report a cyber-security breach. The cyber-security structure must run the cyber-security programme and report progress to the appropriate authority in the municipality. The designated structure must be provided with an adequate budget to implement cyber-security risk mitigation strategies across the municipality.
11.	**I know what to do if I want to report breaches or violations against the cyber-security policy** (a) Why it is important to have a cyber-security call centre/helpdesk Users/employees must know where to report suspected cyber-security breaches or cyber-security policy violations. A central cyber-security reporting centre assists with collecting comprehensive statistics on the types of cyber risks that the municipality is exposed to. Cyber-security call-logging assists with the prioritisation of the reported issue and tracks it down to its resolution. With appropriate skills, helpdesk centre staff provide necessary guidance on how to respond to a cyber-security incident and this helps to contain the possible spreading of the reported cyber-security incident. (b) Risks associated with the absence of a cyber-security call centre/helpdesk Absence of a cyber-security call centre leads to confusion about where to report suspected cyber-related incidents. Absence of a cyber-security helpdesk is a motivating factor for employees not to report cyber incidents, hence it becomes difficult to manage cyber-security incidents at an early stage before the issue/situation can spread across the entire organisation or to certain critical information infrastructure assets. Absence of a cyber-security call centre makes it difficult to keep trends and analyse reported incidents for future planning and informed decision making on enhancing cyber-security in the municipality. (c) Recommended practice for cyber-security call centre/helpdesk

	There must be a cyber-security call centre that operates 24/7 as some information infrastructures need to be kept operating all the time. The call centre must have appropriately skilled resources. The call centre must have a bird’s eye view of all critical information infrastructure assets to ensure business continuity of such critical assets. The call centre must keep and maintain records pertaining to reported issues and incidents.
12.	**I know who the custodian of the cyber-security policy is** (a) Why it is important to have a designated custodian of the cyber-security policy The cyber-security policy needs to be continuously reviewed in order to remain relevant in the fast paced technology advancement environment in which the municipality is participating. Custodianship ensures that cyber-security is reviewed and approved by the appropriate authority. Knowing who is responsible for cyber-security enhances the level of contribution to improve the contents of the policy. The custodian of the cyber-security policy is the structure that must be responsible for cyber-security awareness initiatives. The custodian must ensure that the policy is well communicated to the employees, and employees must acknowledge and declare their understanding of the cyber-security policy. (b) Risks associated with not knowing who the custodian of cyber-security policy is? There could be minimal contribution from the key stakeholders on the contents of the policy. There could be lack of ownership and accountability regarding the cyber-security policy. The cyber-security policy could be dormant and hence not contributing to advancing the cyber-security agenda in the municipality. (c) Recommended practice from the custodianship of the cyber-security policy There must be a custodian of the cyber-security policy. The custodian is responsible for continuously updating the policy document. The custodian is responsible for communicating the contents of the policy across the organisation and also for monitoring compliance with the policy.
13.	**My organisation conducts research and development with the aim to enhance protection of the information infrastructure** (a) Why research and development is important in the advancement of information infrastructure protection Co-ordinated management of research and development on cyber-security and information infrastructure protection promotes the advancement of protecting the information infrastructure against cyber risks. Research and development promotes cyber-security alignment to current trends in the cyberspace. Outdated protection mechanisms compromise cyber-security and hence protection of critical information infrastructures.

(b) Risks associated with the lack of cyber-security research and development

There could be a heavy/extensive dependency on external institutions to provide insight and advice on the advancement of cyber-security initiatives in the municipality. This dependency might be very costly to the municipality. This dependency can be exploited for business gains and become a fertile environment for fraud and corruption, thereby compromising information infrastructure dependency.

(c) Recommended practice for the research and development towards the advancement of information infrastructure protection

A budget must be allocated for research and development in pursuit of safeguarding the information infrastructure. Cyber-security implementation must be informed by research and development in the municipality. There must be collaboration with appropriate stakeholders, including other spheres of government, vendors, and tertiary education institutions. Employees must be allowed to join professional institutes and to attend relevant conferences, workshop, and seminars.

14. **Protection of information infrastructure in my organisation is guided by the industry best practices**

(a) Why industry best practices are important in protecting information infrastructures against cyber-threats

Adoption of industry best practices promotes appropriate safeguarding of information infrastructure assets, particularly critical information infrastructures, against cyber threats. Protection mechanisms that are recommended by the industry standards have been tested and proved to be working in general. Industry good practices provide/offer guidance on how to implement effective controls to secure the critical assets. The industry practices include Cobit, and various ISO standards that are applicable to cyber-security, and critical information infrastructure such as ICT. There are also standards that are applicable to PCS.

(b) Risks associated with non-adoption of industry best practices in safeguarding information infrastructure

Protection of information infrastructure could be compromised due to the use of unverified/untested cyber-security mechanisms. There could be a lack of direction in pursuit of protecting information infrastructure assets. It could be difficult to involve vendors and service providers because they might not be familiar with the adopted practices if they are not in line with industry best practices. Systems downtown could be prolonged due to limited exposure to organisational specific practices which might be against the known and well adopted industry practices. There could be a risk of depending on a few individuals within the organisation who are the only people who know the organisational practices. These few individuals might hold the

	municipality to ransom. There could be duplication of efforts and costly processes to protect the information infrastructure. (c) Recommended practice for the adoption of industry best practices in pursuit of information infrastructure protection There must be co-ordinated efforts to adopt industry best practices to protect information infrastructure assets against cyber risks. A budget allocated to advance the adoption of industry practices is necessary. If required, relevant resources must be trained in adopting/implementing international/best industry standards. There must be standardised adoption of such industry practices. For all ICT-related activities or functions, there must be an adoption of specific best practices consistently across the organisation. For PCS processes, it is necessary to consistently adopt best practices. There must be uniformity in the adoption of best practices within the Municipality. Compliance to industry best practices must be monitored and audited frequently, at least once a month.
CYBER-SECURITY GOVERNANCE DOMAIN	
15.	**My organisational strategic risk register contains cyber-security risk** (a) Why it is important to include cyber-security risks in the strategic risk register An approved strategic risk register is an important tool used by management amongst other things to allocate funding/budget for the implementation of risk mitigation strategies. If cyber-security risk forms part of strategic risk, it becomes easier for management to allocate the necessary resources. Strategic risks receive appropriate management consideration and priority. (b) Risks associated with exclusion of cyber-security from the strategic risk register There could be lack of executive support. The cyber-security agenda could not be elevated to strategic level. The Cyber-security strategy could be misaligned with the municipal IDP. There could be lack of sponsorship on cyber-security initiatives. Could not be audited as audits are risk based. (c) Recommended practice for the inclusion of cyber-security in the strategic risk register Cyber-security risk must be included in the strategic risk register. Due to the possible impact of cyber-security breaches of municipal operations and mandate, cyber-security risk must be elevated to the strategic level. Including cyber-security in the strategic risk register ensures that cyber-security will be audited as internal audit plans are risk based.
16.	**Management has allocated adequate budget to implement the cyber-security policy** (a) Why allocating budget to implement the cyber-security policy is important

	The cyber-security policy must be of high quality in order to properly articulate the municipal position on cyber-security. The policy must cover all information infrastructure assets within the organisation and therefore must be a comprehensive and well researched document. In order to cover all the necessary areas, the policy must be developed by skilled people. Therefore, necessary funding must be made available to drive the advancement of the cyber-security policy. The cyber-security policy must be marketed and communicated across the municipality – all these activities require some form of sponsorship and hence the need for allocating budget for this item. (b) Risks associated with non-allocation of budget in implementing the cyber-security policy The cyber-security policy could not serve its purpose if it does not address all key areas in the protection of information infrastructure. Protection of critical information infrastructure could be compromised because activities that are embedded in the successful implementation of the policy might not be funded and not executed/actioned. The cyber-security policy could be dormant due to lack of sponsorship to assist with the support necessary for continuously updating, reviewing, and communicating the policy across the municipality. Lack of budget could frustrate the implementation of the cyber-security strategy. (c) Recommended practice for the allocation of adequate budget to advance cyber-security policy implementation Management must allocate adequate budget in order to implement the cyber-security policy across the municipality. To implement the cyber-security policy, there must be a proper cyber-security strategy. Therefore, funding the implementation of the cyber-security policy promotes the safeguarding of information infrastructure assets. Allocation of a cyber-security policy implementation budget must be commensurate with the protection expected for critical information infrastructure assets
17.	**Risk management processes guide the implementation of cyber-security controls in my organisation** (a) Why risk management processes are essential in implementing cyber-security controls Cyber-security risks must be appropriately mitigated in order to ascertain that organisational objectives and mandates are achieved. The rationale for resource allocation could be difficult to justify if cyber-security does not incorporate or is not covered in the risk management processes in the municipality. Risk management processes elevate the agenda of cyber-security and justify the provision of a budget and other forms of resources allocation.

	(b) Risks associated with cyber-security that is not aligned to risk management processes There could be lack of management buy-in and to provide the much needed sponsorship. Cyber-security implementation could prove difficult to justify its existence. It could also be difficult to raise the cyber-security agenda to executive management level. Cyber-security risks have the potential to halt delivery of essential services. This could lead to loss of life and other forms of loss and or devastating consequences. (c) Recommended practice for aligning cyber-security to risk management processes Cyber-security must be aligned to risk management processes in the municipality. Implemented cyber-security controls must be continuously tested/evaluated to provide assurance that they mitigate the risks that they were implemented to mitigate. Risk assessment must be conducted on cyber-security, and on information infrastructure.
18.	**Management has provided guidance on the regulatory requirements pertaining to the information infrastructure that I work with** (a) Why management must provide guidance on information infrastructure regulatory requirements There are regulatory requirements that the municipality must abide by in pursuit of their constitutional mandate of service delivery. These regulatory requirements prescribe minimum requirements on operating information infrastructure. These regulatory requirements include various ICT Acts. (b) Risks associated with non-conformance with applicable regulations There could be information security compromise leading to cyber-security breach/violation. There could be exposure to litigations due to breaches of various laws. (c) Recommended practice for regulatory requirement pertaining to information infrastructure The municipality must compile a list of all applicable Acts and subsequently check compliance with those laws continuously. There must be user awareness campaigns for all the identified Acts.
19.	**Management has allocated adequate people to protection information infrastructures** (a) Why allocating adequate people to safeguard information infrastructure is important People are the most important assets in the organisation. It is essential to allocate sufficient people to strengthen the cyber-security protection of the information infrastructure. People operate technology and information infrastructure to advance

	the organisational mandate. Allocating adequately means having enough people to work on the cyber-security policy, and monitoring the implementation of the policy. Having enough people means there are sufficient people working on cyber-security user awareness, working at the cyber-security call centre or helpdesk, to ensure cyber-security strategy implementation as a whole. (b) Risks associated with inadequate people allocated to information infrastructure protection Without enough people to execute the required activities for protection of information infrastructure, safeguarding of these assets could be compromised. There could be serious issues with people working overtime and could result in disgruntled employees, with low morale. (c) Recommended practice for the allocation of adequate people to safeguard information infrastructure assets. Management must allocate adequate people to the activities that must protect the municipal information infrastructure. Allocation of people must be commensurate with the level of protection required/expected. The number of people allocated must be continuously reviewed in order to be aligned with the evolution in the protection of information infrastructure.
20.	**Management enforces compliance with cyber-security** (a) Why enforcing cyber-security compliance is important Enforcing compliance is a form of monitoring and controlling the cyber-security activities. Enforcing compliance assists management in ensuring that people/employees comply with applicable policies, and it reassures them that organisational objectives could be achieved and sustained. Enforcing cyber-security compliance inculcates the culture of cyber-security in the municipality, thereby advancing the safeguarding of critical information infrastructure. (b) Risks associated with non-enforcement of compliance to cyber-security People are the weakest link in protecting information infrastructure. They need to be reminded all the time of what the organisation expects with regard to their role in cyber-security activities. Without compliance there could be no safeguarding of information infrastructure. Areas that need management attention would be difficult to identify early enough when it might be cheaper to address. It could be difficult to run a successful cyber-security programme without compliance. (c) Recommended practice for enforcing compliance to cyber-security Management must plan and schedule time to conduct testing of compliance with the cyber-security policy on information infrastructure. There must be a budget allocated to testing and enforcing cyber-security compliance. After compliance testing, there

	must be a report to senior management detailing the outcome of the compliance testing exercise.
21.	**In my organisation there are oversight structures/committees that hold management to account for the protection of information infrastructure** (a) Why oversight committees are important in safeguarding information infrastructure The oversight committee holds management to account for the internal controls that have been implemented to mitigate the risks that have been identified in the municipality. These committees enhance the cyber-security, and the identification of areas that require management attention. If working properly, these committees enforce/promote consequence management on breaches and non-performance. Oversight reports also provide authority to allocate necessary resources to achieving organisation objectives. (b) Risks associated with the lack of oversight committees Consequence management could be compromised. There could be no checks and balances implemented to determine if management are working or not. There could be no accountability on the side of management, which might have a negative ripple effect on achieving municipal objectives. (c) Recommended practice for oversight committees on safeguarding of information infrastructure There must be oversight committee(s) for the information infrastructure. These committees must meet at least quarterly to discuss the affairs of their portfolios. These committees include the audit and risk committees, the infrastructure committee and Exco. Because cyber-security is in the strategic risk register, there must be close monitoring of the mitigation controls that management has implemented to deal with the associated risks.
22.	**Internal audit operational plans incorporate audits or reviews on information infrastructures on an annual basis** (a) Why it is important for the audit plan to incorporate audits on information infrastructure Independent and objective assurance in appraising the design and effectiveness of controls implemented by management is essential in ensuring that the municipality achieves and sustains its mandate. Therefore these objective and independent appraisals must include information infrastructures. Since internal audit plans are risks based, it becomes easier to include information infrastructure if cyber-security is covered in the risk management processes and included in the strategic risk register.

	(b) Risks associated with the exclusion of information infrastructure in the internal audit plan There could be assurance that internal controls around the protection of information infrastructure are working as intended by management. The audit and risk committees would not provide the necessary oversight on information infrastructure. Control deficiencies might not be properly interrogated and subsequently hold management to account for and committed to correcting those control deficiencies. Control deficiencies in information infrastructures could have devastating consequences in the function of the municipality as a whole. (c) Recommended practice for including information infrastructure in the internal audit annual operational plan Auditing information infrastructure must be a line item in the internal audit annual operational plan. The time allocated to conduct the audit on information infrastructure must be aligned to the complexity of the assets to be audited.

23.	**Management has input in the internal audit operational plan before the plan is implemented** (a) Why it is important for management to have input in the internal audit operational plan Management is responsible for implementing systems of control in the municipality. Management knows how controls ought to be designed and implemented. Therefore it is essential for management to have input in the internal audit plan in order to offer the necessary advice on the completeness of areas to be tested during the audit process. Engaging management improves cooperation during the audit processes, and also prepares management for the audit. (b) Risks associated with exclusion of management involvement before the audit operational plan is implemented There could be a lack of the much needed support to be provided to the audit team (there could be no buy-in by management). Lack of management involvement in preparing the annual audit plan could frustrate the execution of the audit process. Audit efforts could be directed at less important areas. There could be wastage of resources if management believes that the audit was focusing on irrelevant areas. (c) Recommended practice for management involvement in preparation of the annual audit plan Management must be consulted before the internal audit plan can be put into operation. Co-operation of management is essential when auditing the controls in the organisation. Management must have input on the timing of the audit process and they must have input in the scope of the audit.
24.	**Audit committee approves the internal audit operational plans before the plan is implemented** (a) Why it is important that the audit committee approves the audit operational plan before being implemented Internal audit reports functionally to the audit committee. The audit committee ensures the independency of the internal audit committee. Members of the audit committee are not employees of the municipality and hence the independence of the internal audit function. By approving the internal plan, the audit committee confirms that the audit coverage is comprehensive and covers most of the high priority areas and high risk areas. The audit committee monitors the implementation of the plan it has approved. (b) Risks associated with non-approval of the audit plan by the audit committee The focus of the audit plan might not be comprehensive and directed at priority areas. The committee might not provide the required oversight on the implementation of the plan. Independence of the internal audit function could be compromised.

	(c) Recommended practice for the approval of the internal audit operation by the audit committee The internal audit operational plan must be approved by the audit committee to enhance and sustain the internal audit's independence and objectivity. Once approved, the internal audit function must report at least quarterly to the audit committee on the progress of operational implementation.
25.	**Management has implemented clear asset management practices** (a) Why it is important for management to implement asset management practices Some of the information infrastructure assets in the municipality support the provision of essential services and other types of critical infrastructure. Therefore it becomes essential that proper asset management principles are adopted to ensure that continuous provision of essential services is not compromised/disturbed. Asset management practices ensure that there is proper acquisition of information assets, there is a proper maintenance plan for critical infrastructure assets, and there is proper disposal of old or unwanted assets. (b) Risks associated with the lack of clear asset management practices There could be delays in the acquisition of critical information infrastructure assets which could negatively impact business continuity. There could be no proper maintenance plan for critical information infrastructure which could result in challenges to sustain business continuity. Information infrastructure assets could be disposed inappropriately, thereby exposing the municipality to information security risks. (c) Recommended practice for implementing asset management practices Municipality must implement asset management practices to guide the management of information infrastructure assets. At least an inventory of critical information infrastructure must be at the core of such asset management practices. There must be a designated structure to ensure that critical information infrastructure assets are appropriately managed through the adoption of appropriate asset management practices.
26.	**Management understands the possible impact of cyber-security threats to municipal service delivery** (a) Why it is important for management to understand the possible consequences of cyber threats to municipal operations? Understanding of the possible impact of cyber-security breach or violation is essential for management because their effort to safeguard information infrastructure would be commensurate to such possible impact. Management understanding of possible impact serves as a motivating factor to acquire their buy-in, sponsorship, and other various forms of support.

	(b) Risks associated with management not understanding possible consequences of cyber-security breach/violation There could be inadequate allocation of resources to support the cyber-security agenda. Cyber-security can be left in the hands of an individual, thereby compromising its functionality. There could be sponsorship for the cyber-security programme. The cyber-security programme may not align with the municipal IDP. Management could view cyber-security as an 'add on' or nice to have as opposed to it being viewed as an investment, and critical tool to ensure continuity of the municipal business. (c) Recommended practice for management understanding of possible consequences of cyber-security breach/violation Management must be informed of the possible consequences of cyber-security breaches so that they can commit and provide the necessary support to implement appropriate risk mitigating controls. A cyber-security designated structure must ensure that management is made aware of possible consequences through user awareness sessions. Audit reports must also alert management to the possible consequences that could results from deficiencies in the systems of internal controls.
CYBER-SECURITY TECHNICAL OPERATIONS DOMAIN	
27.	**There are service level agreements between my municipality and the service providers working on information infrastructures** (a) Why it is important that there are service level agreements between the service providers and the municipality Working on information infrastructure requires 24/7 available of support due to the dependency of the Municipal business process on such infrastructures. Therefore there must be a working relationship that ensures that necessary support will be available as and when required by the Municipality. Also working on information infrastructure requires high degree of confidential and trustworthiness. Therefore it is essential that there are service level agreements in place for all service providers that are working on information infrastructure assets. (b) Risks associated with the lack of service level agreements Municipal business continuity could be compromised as some of the critical services are provided by services providers who are not controlled by the municipal policies. It could be a challenging or daunting task to hold service providers accountable in case of non-performance and or cyber-security violation on their part without service level agreements. (c) Recommended practice for the service level agreement There must be an appropriate service level agreement for each outsourced service on information infrastructure. The service level agreement must be appropriately

	compiled by management with the involvement of the municipal legal services unit. In order to be enforced, a service level agreement must be signed by both parties, which in this case are the municipality and the service provider.
28.	**Management is monitoring the services provided by the service providers/consultants against the service level agreements** (a) Why it is important to monitor service providers' performance against the service level agreement Service level agreements serve as a motivation to service providers to perform according to the municipal expectations. Monitoring service level agreements enforces the service provider to deliver their services as required by the municipality. Monitoring service level agreements also advances business continuity of the outsourced services. (b) Risks associated with the lack of service level agreement monitoring Outsourced services might not be delivered as expected by the municipality, and subsequently business continuity could be compromised. Service providers can charge for services that they have not performed, leading to financial loss by the municipality. Poorly performing service providers can continue to conduct business with the municipality despite their poor performances. (c) Recommended practice for monitoring service level agreements Management must monitor service level agreements on all outsourced services on information infrastructure. Service level agreements must contain punitive clauses in case of non-performance and or breach of trust by the service provider. The reports on service level agreements must be shared with/communicated to the supply chain management function in order to be officially communicated with the service provider, and for future reference purposes.
29.	**My organisation has deployed technologies to protect information infrastructures against cyber threats** (a) Why it is important to deploy automated technologies to safeguard information infrastructure Appropriate automated technologies are effective and efficient in detecting cyber threats, prevent threats to access information infrastructure, and monitor activities on information infrastructure. These automated technologies perform activities that human beings cannot perform. By their very nature, information infrastructure assets require automated technologies to be protected. Physical security is also important. If appropriately implemented, automated technologies offer 24/7 protection, and monitoring of information infrastructure assets.

	(b) Risks associated with lack of automated technologies to safeguard information infrastructure Besides physical security, information infrastructure requires only automated technologies in order to be protected. Without automated technologies, infrastructure assets would not be protected and would be exposed to cyber threats. (c) Recommended practice for automated technologies to protect information infrastructure The designated cyber-security function must implement current and applicable automated technologies to safeguard information infrastructures. This goes hand to hand with asset management practices. Automated security technologies must be deployed and implemented for all critical information infrastructure assets within the municipality. The designated cyber-security structure must keep an inventory of all automated technologies implemented in each information infrastructure asset.
30.	**Access to information infrastructures is controlled through identification and authentication** (a) Why it is important to control access through identification and authentication Keeping track of and records on the activities on information infrastructure is important because it provides evidence of who accessed the resource, and furthermore in other cases, it aligns the actions performed on the resources by the individuals, thereby confirming accountability behind those actions that have been performed. User identification ensures that the municipality knows who the individual is that accessed the infrastructure asset. Knowing who the individual is, is not sufficient. That individual must confirm whether they are the person. They must prove that they are indeed the one purported to be them. (b) Risks associated with lack of identification and authentication of users when accessing information infrastructure There could be uncontrolled access to information infrastructure, thereby compromising the protection of such assets. Uncontrolled access could lead to unauthorised modification of information assets, and also could lead to lack of accountability. If you cannot identify who performed certain activities on information infrastructure, it also means that you cannot hold anyone accountable for such activities. (c) Recommended practice for user identification and authentication when accessing information infrastructure assets There must be proper identification and authentication mechanisms for all users who access information infrastructure assets. There must be a unique identification for each user in order to enforce accountability.

31. **Management has adopted industry best practices to protect information infrastructure against cyber-threats**

(a) Why it is important to adopt industry standards to secure information infrastructure

At an operational level, industry standards are widely known and used by various institutions, and if the municipality adopts these widely known standards, support of information infrastructure that uses those standards becomes easily available. The standards are universal tools that achieve consistency in the application of information infrastructures. Service providers who are known and understand these universal standards have an advantage when providing support to information infrastructure assets. Industry standards offer credibility for the work done on the information infrastructure, only if they have been used to such work. Industry standards offer critical and credible guidelines to be adopted by the municipality when safeguarding the information infrastructure

(b) Risks associated with non-adoption of industry best practices/standards

Organisational siloed processes could be adopted to protect the information infrastructure which could prove to be costly and unreliable. Organisational siloed processes could be difficult to outsource and or to be supported by service providers. It could be difficult for management to rely on the effectiveness of controls implemented without reference to industry best practices or standards. There could be lack of direction and insight without the guidance of industry best practices

(c) Recommended practice for the adoption of industry best practices

The cyber-security designated structure must develop an inventory of industry standards that can be adopted by the municipality for each type and use of information infrastructure. The rationale for a selected standard must be clear and communicated to relevant management. Once a specific industry best practice has been adopted, compliance to such a standard must be monitored and enforced.

32. **Anti-virus software is installed on our laptops, desktops, and other devices**

(a) Why it is important to use anti-virus software for the applicable information infrastructure

Prevention is better than cure because it is much cheaper to implement than fighting fires trying to contain the spread of the virus in the information infrastructure system. Anti-virus software is used as a proactive mechanism to prevent known viruses from infecting the information infrastructure. Implementing anti-virus software is a risk mitigating mechanism, and it limits the possibility of the information infrastructure becoming infected with viruses.

(b) Risks associated with not implementing anti-virus software

	The information infrastructure could be infected by viruses, thereby compromising information security. It could be costly to fix the information infrastructure once infected by viruses. There is also a possibility of disturbance/disruption to service delivery. (c) Recommended practice for the implementation of anti-virus software The cyber-security designated structure must ensure that applicable information infrastructure assets are uploaded with the current anti-virus software. Management of anti-virus software must follow appropriate asset management practices. Where applicable, there must be licences for each type and copy of anti-virus software that is used by the municipality.
33.	**Audits are conducted to provide assurance of the adequacy and effectiveness of controls that have been implemented to protect information infrastructure** (a) Why it is important to conduct audits on information infrastructure controls Management must ensure that the business objective is achieved through, amongst others, implementing appropriate risk mitigating controls. Management needs to get assurance on the adequacy and effectiveness of such implemented controls. Auditing these controls is the appropriate mechanism for management to determine if the controls are working as intended. Auditing of controls assists management to identify control deficiencies and offer the opportunity to fix those gaps. Auditing can be conducted by various structures including management themselves, external auditors (Auditor General), internal audit, and the information infrastructure vendors. (b) Risks associated with not conducting the necessary audits Weakness in the implemented controls may not be detected early enough to correct them before being exploited. Auditing is a motivating tool to get all relevant stakeholders to be on their toes when it comes to the effectiveness of controls, and therefore without an audit, monitoring of controls could be compromised and weakening the protection of information infrastructure against cyber risks. (c) Recommended practice for auditing information infrastructure controls Because cyber-security is in the strategic risk register, management must ensure that audits are continuously conducted to test the adequacy and effectiveness of implemented controls in order to identify areas that require management's urgent attention. The results of the audits must be communicated to applicable stakeholders and structures such as the audit and risk committees. Where controls have been violated, consequence management must be implemented, and must be constantly applied.
34.	**The incident management procedures are adequate to resolve cyber-security incidents** (a) Why it is important to have cyber-security incident management procedures

	Cyber-security incident procedures provide guidelines to be followed in cases of emergency or after declaration of a cyber-security incident. Incident management must be continuously tested and various stakeholders must be involved in such testing processes. Incident management procedures make it possible to contain the cyber incident, and get the information infrastructure up and running again in the shortest possible time. Relevant people know what to do in the case of a cyber-incident, and this minimises the information infrastructure down time. (b) Risks associated with the absence of cyber-security incident management procedures There could be confusion about the roles and responsibilities when a cyber-security incident has been declared, and this could prolong the information infrastructure downtime, and also may compromise information security. Containment of the cyber-incident could be difficult to achieve and the situation could escalate if not dealt with in a proper manner as it should be documented in the incident management procedures. (c) Recommended practice for the implementation of cyber-security incident management Cyber-security incident management procedures must be documented and continuously tested by the cyber-security designated structure. Incident management procedures must be audited at least annually in order to be assured that they are continuously relevant to the prevailing conditions of information infrastructures. All critical information infrastructures must be linked or covered by cyber-security incident management procedures.
35.	**The building that I work in is adequately protected to secure the information infrastructure** (a) Why it is important to safeguard the building that houses the information infrastructure? Physical access to the building that contains the information infrastructure must be adequately controlled. Uncontrolled access to the building could compromise information infrastructure protection. There could be theft of information infrastructure which could expose the municipality to information security risks. Spying devices could be implanted in the building, thereby compromising the safety of the information infrastructure. It is therefore essential that the cyber-security designated structure implements measures to advance the safety of the buildings that house information infrastructures. (b) Risks associated with the unsafe building that houses information infrastructure There could be theft of information infrastructure, thereby compromising business continuity, and exposing the municipality to information security risks. Uncontrolled

	access could expose the municipality to various threats including implanting spying software, and hijacking of employees with the intention of getting access to information infrastructures. (c) Recommended practice for securing the buildings that house information infrastructure All the buildings that house information infrastructure must be properly secured in order to limit uncontrolled access to those buildings. The cyber-security designated structure must create an inventory of all the buildings that house critical information infrastructure, and ensure that access to such buildings is controlled. Depending on the housed information infrastructure, the type of security to be implemented must be aligned to the importance of the information infrastructure in the building.
MANAGE HUMAN ISSUES IN CYBER-SECURITY DOMAIN	
36.	**Employees' activities on the information infrastructure are monitored** (a) Why it is important to monitor employees' activities on the information infrastructure Municipal information infrastructures must be used only to advance the business interests of the municipality. Due to the susceptibility of the information infrastructure, the cyber-security designated structure must monitor the activities of employees on information infrastructure. Some of the employees' activities could motivate or invite unwanted attention to harmful outsiders. Some employees' activities on information infrastructure can expose the municipality and its resources to cyber ills and risks and hence the control and monitoring is essential. (b) Risks associated with uncontrolled and or unmonitored employees' activities on information infrastructure There could be unauthorised usage of municipal bandwidth which could impact the performance of the information infrastructure. Some activities could expose organisational assets to information security risks. Employees' access and activities on social media and related platforms must be appropriately controlled because they can divulge sensitive organisational resources and information. Accessing a rogue harmful website can introduce dangerous viruses and other cyber-ills to the municipal information infrastructure. (c) Recommended practice on monitoring employees' activities on information infrastructure Cyber-security policy must be clear on the acceptable use of information infrastructure. The cyber-security designated structure/function must deploy automated tools to monitor and control employees' activities on the information infrastructure.

37.	**In my organisation action is taken against employees who violate cyber-security policy** (a) Why it is important to take action against employees who violate cyber-security policy The consequences associated with breach of cyber-security could be devastating and therefore management must take a decisive position on addressing violations to cyber-security policy. The action taken against the culprit employees must be aligned to the consequence and or possible consequence of the exposure due to the security breach. Taking action inculcates the culture of cyber-security in the municipality. Action to be taken is not only limited to punitive measures but it can also include training and awareness. (b) Risks associated with not taking action against the employees who violate cyber-security policy There could be no consequence management on the employees that violate cyber-security policy. If action is not taken, other employees could be motivated to do similar acts in the future and it will be difficult to hold them accountable as the precedence had already been set. It could prove to be difficult to instil the required culture of cyber-security. (c) Recommended practice for taking appropriate actions against employees who violate cyber-security policy. Management must ensure that employees are aware of what is expected of them when working on information infrastructure. Management must satisfy themselves that employees are aware of the cyber-security policy. Breaches to cyber-security policy must be properly investigated by a competent structure. If it is confirmed that the cyber-security policy has been breached, then management must take appropriate disciplinary actions against the involved employee. The results of the disciplinary action must be shared with relevant employees in order to serve as a motivation not to commit similar acts.
38.	**Employees are made aware of the cyber-security policy contents** (a) Why it is important to educate employees on the cyber-security policy contents The cyber-security policy states the position of the municipality in securing the information infrastructure. The designated cyber-security function must educate employees on cyber-security content to make them aware of and to understand what is expected from them when working on the information infrastructure. If the cyber-security policy has not been properly communicated to employees, enforcement to comply with such a policy can be a challenging task if not a futile exercise. (b) Risks associated with not educating employees on the contents of cyber-security

	Normally employees are busy with their duties as detailed in their job descriptions. If employees are not trained in the contents of cyber-security that are essential and relevant to the type and nature of information infrastructure that they are operating, they are prone to make honest mistakes and be negligent when performing their duties. If employees have not been educated on the contents of cyber-security, it would be difficult to enforce compliance with such a policy. It could also be difficult to hold employees accountable and take action against them in case of cyber-security violation. (c) <u>Recommended practice for educating employees on the contents of cyber-security policy.</u> The designated cyber-security structure must educate employees on the contents of the cyber-security policy that are relevant to the types and nature of information infrastructure being operated or used by the employees. After conducting such an education exercise, employees must be required to acknowledge receipt of such education/training and must be required to sign the attendance register after those training sessions. Changes to cyber-security policy must be appropriately communicated to the affected employees
39.	**Employees know where to report suspicious illicit cyber-security activities** (a) <u>Why it is important for employees to know where to report suspicious illicit cyber-security activities</u> Employees are the eyes and ears of the municipality. Therefore it is important to report suspicious activity that could disturb or interrupt the normal function of the municipal business processes including information infrastructure. If the employees know where to report the cyber illicit activities, they are motivated to report such activities. They are also motivated to report such activities as soon as possible, thereby minimising the possible impact of such illicit activity. (b) <u>Risks associated with employees not knowing where to report suspicious illicit cyber activities</u> There could be delays in reporting dangerous and harmful activities that could harm and or destruct the normal operation of the information infrastructure. The delays in reporting could lead to escalation of the harmful activity. Normally delays are proportionately associated with costs. Not knowing where to report incidents could be very costly to the municipality. (c) <u>Recommended practice for making employees aware of where to report suspicious illicit cyber activities</u> The designated cyber-security structure must invest in making users/employees aware of what to do and where to report suspicious illicit cyber activities. Employees must be encouraged to report such activities as soon as possible after identifying

	them. Employees must be made aware that they can also report such activities anonymously if they are uncomfortable to disclose their identities.
40.	**Employees receive adequate training in the information infrastructure they operate** (a) Why it is important for employees to be trained in the information infrastructure that they operate It is essential that employees are trained in how to operate the information infrastructure because they can make costly errors that could expose the municipality to information security risks. Therefore, training is a control that eliminates or limits the number of honest errors that could be committed by employees. Inappropriate use of the information infrastructure could also expose the municipality to cyber threats. (b) Risks that are associated with not training employees in the information infrastructure that they operate Information infrastructure could be exposed to cyber ills such as unknowingly disclosing the IT system's access credentials to strangers or unauthorised personnel. Lack of training can also compromise information security where employees unknowingly protect their system credentials with weak passwords or even sharing their credentials with their colleagues. Also, system administrators may not perform hardening of hardware and operating systems before implementation. Network administrators must be trained to conduct vulnerability assessment in order to identify network exposures to cyber threats. (c) Recommended practice for training employees in the information infrastructure that they operate Management must continuously train employees in the information infrastructure that they operate or are exposed to. Employees must be allowed to attend conferences, workshops, seminars and other training-related activities that are pertinent to the information infrastructure that they operate. Attending such training activities will keep them updated with the current trends impacting on those infrastructures.
41.	**I am aware of cyber-security threats affecting the information assets I work with** (a) Why it is important that the employees are aware of cyber-security threats affecting the information assets that they operate It is essential that each employee is aware of possible cyber threats that could affect the information assets because they can determine the early warning of such threats or the employee can act accordingly to minimise exposure to such threats. It becomes

	easier for employees to protect something because they know to prevent it in the first place. (b) Risks associated with employees not knowing of the cyber-security threats that may affect the information assets they work with Employees are the weakest link in information infrastructure protection. Employees' behaviour can encourage some cyber-security threats to exploit the vulnerability if they are not aware of those threats. Employees' behaviour and attitude can perpetuate some cyber-security threats. Not knowing the threats is fertile environment for the threats to exploit the vulnerabilities. If employees are not aware of threats, there is a large possibility that the exposure or vulnerabilities that can be exploited are not known as well, thereby compromising the security of information and related infrastructure. Employees could be inadequately prepared to behave in a manner that would limit the likelihood or impact of such threats. (c) Recommended practice for employees to know the current trends in cyber-security threats that could impact on the information infrastructure that they work with The designated cyber-security structure must conduct research continuously and or collaborate with relevant stakeholders in order to enhance knowledge on the current trends in the threats that could affect the municipal information infrastructure. The current trends must be properly communicated with all relevant employees in order to make them aware of the risks. Information on the threats must be continuously disseminated to relevant employees in order to sensitise them to act and behave in a manner that would limit the risk exposure.
42.	**I am aware that organisational internet and e-mail systems should be used for business purposes** (a) Why it is important that employees are aware that the organisational information infrastructure must be used for business purposes Municipal information infrastructure such as the internet and e-mail systems must only be used for conducting municipal business. Any other use besides the official use could invite dodgy characters to interact with the employee. People using the Internet and e-mail can hide their characters and activities that could later be harmful to business operations of the municipality. (b) Risks associated with not utilising municipal internet and e-mail systems for official business only Other activities besides the official ones can be a fertile environment to engage with criminals which could exploit information security vulnerabilities. Internet and e-mail systems are the major sources of cyber ills/threats.

	(c) Recommended practice for use of municipal internet and e-mail systems by employees The designated cyber-security structure must ensure that users are educated on the acceptable use of the municipal internet and e-mail systems. There must be a compulsory awareness/training session on the acceptable use of these systems, facilitated by the designated cyber-security structure.
43.	**Employees accept responsibility for information infrastructure protection** (a) Why it is important that employees accept responsibility to safeguard information infrastructure Employees must take ownership of protecting the information infrastructure because they are the ones who are operating these assets. If they take ownership, they will possibly be committed to protect these assets. Accepting responsibility implies that they will go an extra mile to equip themselves to protect information infrastructures. They can even propose training that is relevant to advance the securing of the information infrastructure. (b) Risks associated with lack of employees' responsibility to safeguard the information infrastructure Lack of responsibility from employees could compromise information security in the municipality. The cyber-security culture may be compromised. There could be lack of commitment to protect the information infrastructure. User awareness campaigns and related training and education could be a challenge to implement. Employees may not attend such educational efforts. (c) Recommended practice for employees to accept responsibility towards securing information infrastructure Protecting information infrastructure must be part of the performance assessment system. Employee duties must explicitly require them to protect the information infrastructure from cyber threats. Performance assessments must be conducted continuously in order to identify areas that require improvement. If gaps are identified in performing duties, appropriate training must be provided to the employee.
44.	**My organisation constantly conducts cyber-security assessment to determine how employees are complying with the cyber-security policy** (a) Why it is important to continuously perform cyber-security assessments The municipality must continuously conduct cyber-security assessment in order to strengthen the controls that are implemented to address the cyber-security challenges. These assessments must be driven by the designated cyber-security structure to test employees' commitment and understanding of the cyber-security policy. Assessing cyber-security is a tool to determine the as is with the intention of

	enhancing the posture of cyber-security. Assessing cyber-security is a form of management communication and commitment to cyber-security (b) Risks associated with not constantly performing cyber-security assessment The level of user understanding and commitment to cyber-security could not be determined. Control weakness may not be identified until it is exploited by the threats. A comprehensive view of cyber-security controls that have been implemented may be difficult to accomplish. (c) Recommended practice for continuously assessing cyber-security Cyber-security assessment must be continuously conducted by the cyber-security designated function. Cyber-security assessment must be conducted on all critical information infrastructure, and the assessment results must communicated to all relevant stakeholders. Cyber-security assessments must be based on or align to cyber-security policy, industry best practices that are relevant to the infrastructure being assessed, and the cyber-security implementation strategy.

7.4. CHAPTER SUMMARY

The cyber-security research instrument was discussed in detail. The rationale behind each statement in the assessment was explained in detailed. The comprehensive details that have been provided in this chapter will provide guidance to the metropolitan municipalities when conducting the cyber-security status assessment to understand the assessment results and implications of the cyber-security control deficiencies.

CHAPTER 8
PROCESS FOR ASSESSING CYBER-SECURITY STATUS

8.1. CHAPTER INTRODUCTION

The main question that this enquiry sought to address was, what is the cyber-security status in the metropolitan municipalities in South Africa? An assessment tool to assess the cyber-security status was developed and was presented in in Chapter 7. The researcher developed a survey questionnaire that was used as an assessment tool to assess cyber-security status. A survey questionnaire was particularly attractive to the researcher because the costs are relatively low and such a questionnaire can reach a large number of participants.

8.2. STUDY SITES

The focus of the research was on the metropolitan municipalities in South Africa, of which there are currently eight in the country. The researcher was able to receive permission to conduct this study at only three metropolitan municipalities, namely eThekwini, Tshwane, and Nelson Mandela Bay.

8.2.1. Tshwane Metropolitan Municipality background

Tshwane Metropolitan Municipality is a category A Municipality. The city of Tshwane is located in Pretoria, the capital City of the Republic of South Africa. This metropolitan municipality covers 6345km² and is reported to be the third largest city in the entire world behind New York, and Tokyo/Yokohama (City of Tshwane, 2017). Tshwane Municipality is located in the Gauteng Province, which is one of the nine provinces in South Africa. This metropolitan municipality is one of the three metropolitan municipalities that are located in Gauteng Province. Tshwane Municipality occupy 30% of 19055 km² land of the Gauteng province.

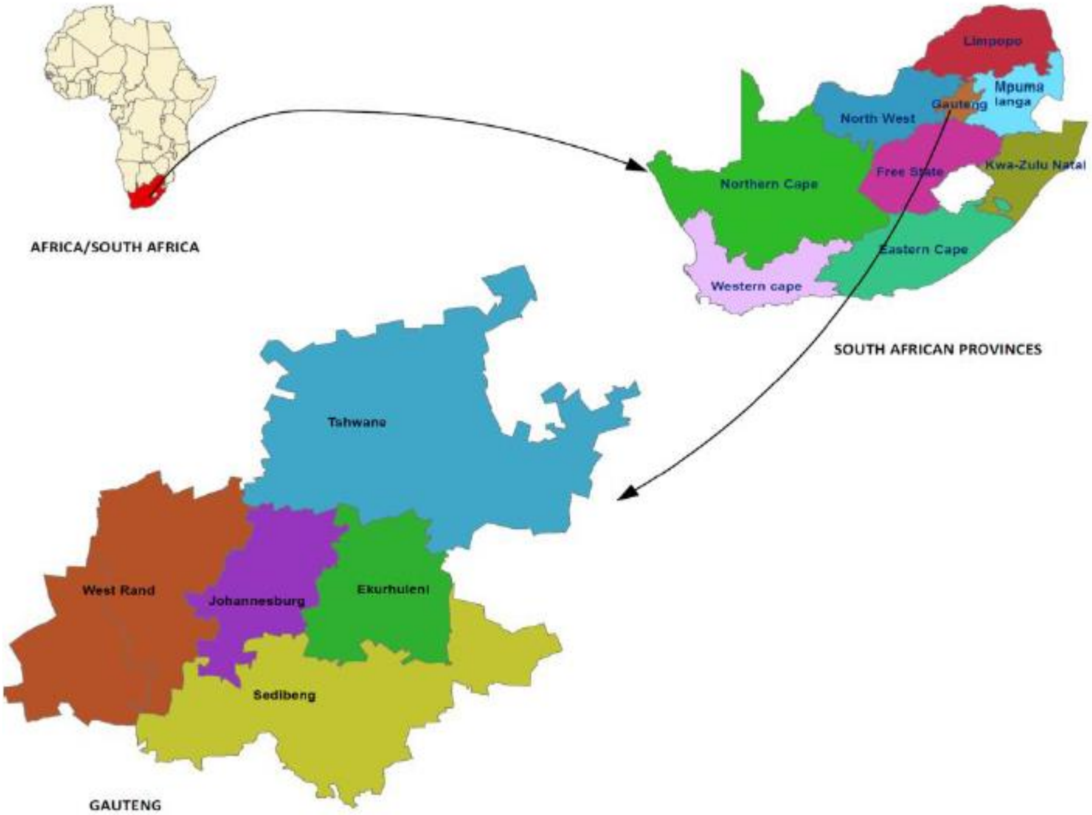


Figure 8.1: Tshwane Metropolitan Municipality in Gauteng Province

Tshwane Municipality is the administrative seat of the South African Government, and hosts a number of embassies. This city has various industrial sites, education and research facilities, and office space. Approximately 90% of all research and development in the country is conducted in Tshwane Municipality (City of Tshwane, 2017). According to the 2017/21 IDP of the City of Tshwane Municipality, the population was reported to be 3 161 809 in 2015.

8.2.2. Nelson Mandela Bay Metropolitan Municipality background

The Nelson Mandela Bay Metropolitan Municipality (NMBMM) is located in the Eastern Cape Province of the republic of South Africa. The NMBMM is located in the city of Port Elizabeth. It is one of the two metropolitan municipalities in the province of Eastern Cape. It has administrative offices in Port Elizabeth. The municipality spans an area of 1959, 02 km². The Municipality is the sea port and manufacturing centre for automotive industry (NMBM, 2017). Creating the vibrant and marine sector are the two ports in the city, which are Port Elizabeth harbour and Ngqura. According to the 2017 municipal IDP, the municipality has a population of 1 271 776. The Municipality is reported to be the economy driver of the Eastern Cape province, contributing provincial gross geographic product of 41,81% (NMBM, 2017).

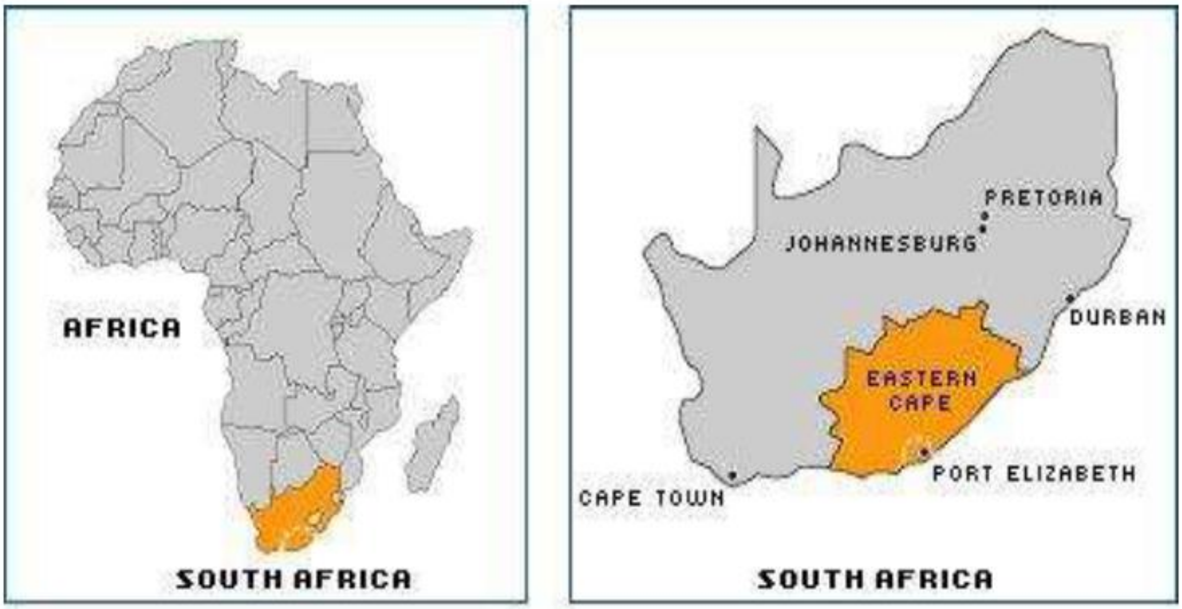


Figure 8.2: NMBM location

Source: Nelson Mandela Bay Municipality (NMBM). 2016. *Integrated Development Plan (IDP) 2016-17–2020/21*. [Online]. Available WWW: http://www.nelsonmandelabay.gov.za/datarepository/documents/adopted-2016-2021-golden-five-years-idp-june-2016-web.pdf.

8.3. THE SURVEY QUESTIONNAIRE

The intention of the survey questionnaire was to collect data from a larger sample, to confirm or dispute what the data uncovered in the ConGTM study. A questionnaire collects data in a survey and it contains questions that require respondents to answer directly on the form without the assistance of the interviewer. The questionnaire was accompanied with a covering letter for the participants which explained the objectives of the enquiry, and contained important information necessary for the completion of the questionnaire. The first part of the survey questionnaire contained biographic details that were used to fragment the data and draw comparisons within the population.

For this enquiry, the researcher opted to adopt e-mail as the tool for delivering the survey questionnaires. An e-mail survey allowed for a larger sample and unlimited geographic coverage. Before the survey questionnaire was deployed to the participants, second ethical clearance was obtained from research office in the University of KwaZulu-Natal.

8.4. SAMPLING PROCEDURE

In some research instances it would be impractical to investigate all targeted populations and hence samples are drawn. Purposive sampling, also known as judgemental sampling, was employed for this enquiry. The study utilised the strategy developed by Onwuegbuzie and Collins (2007) to decide on the enquiry's sample size.

Table 8.1: Minimum sample size recommendations for most common quantitative and qualitative research designs

Study design/method	Suggested smallest sample
Correlational	"64 Interviewees for one-tailed hypotheses; 82 Interviewees for two-tailed hypotheses"
Causal-Comparative	"51 Interviewees per group for one-tailed hypotheses; 64 Interviewees for two-tailed hypotheses"
Experimental	"21 Interviewees per group for one-tailed hypotheses"
Case study	"3-5 Interviewees"
Phenomenological	"≤ 10 interviews; ≥ 6"
Grounded theory	"15-20, 20-30"
Ethnography	"1 cultural group; 30-50 interviews"
Ethological	"100-200 units of observation"

Source: Onwuegbuzie, A. J., & Collins, K. M. (2007). A typology of mixed methods sampling designs in social science research. *The Qualitative Report*, vol. 12, no. 2, p. 289.

The method formulated by Krejcie and Daryle (1970) was adopted to determine the required sample size in each metropolitan municipality. The relevant business units were grouped into three categories, namely Information and Communication Technology, Operation Technology, and Administration. In all the municipalities the response rate was representative.

EThekwini Municipality sample size

Category	Total number of employees	Required sample based on Krejcie and Daryle	Actual responses
ICT	40	36	38
Operating Technology	30	28	29
Administration	60	52	53

Nelson Mandela Bay Municipality sample size

Category	Total number of employees	Required sample based on Krejcie and Daryle	Actual responses
ICT	35	32	34
Operating Technology	40	36	38
Administration	55	48	49

Tshwane Municipality sample size

Category	Total number of employees	Required sample based on Krejcie and Daryle	Actual responses
ICT	35	32	34
Operating Technology	50	44	44
Administration	25	24	24

8.5. THE PILOT STUDY

The researcher pre-tested the survey questionnaire on a small sample. A group of 14 employees were purposively selected, and e-mailed the survey questionnaire. This group represented characteristics of the research target population. The pilot study aimed to understand the reactions of the participants and to make revisions on some questions as guided by the participants' reactions. It is also important to mention that the other aim for the execution of the pilot study was to experiment the cyber-security assessment tool. The researcher wanted to get a feel from the participants whether the survey questionnaire was assessing what it ought to assess. The participants of the pilot study were different from those that participated in the ConGTM. In the actual assessment study, the participants from both the ConGTM study and the pilot study were excluded. The gaps that were identified in the pilot study were addressed by the researcher before the actual deployment of the survey questionnaire to the research population.

8.6. STATISTICAL ANALYSIS

The results of the surveys were analysed using a pre-set indicator for acceptable/good, and unacceptable/bad responses. The good or bad response percentage indicator was pre-agreed with the information management unit and the operating technology team in each participating municipality. Given the low maturity level of cyber-security in the country, a percentage of 55% was a cut-off indicator for good a response. Anything below 55% was regarded as bad for the responses to each question in the questionnaire. It is always necessary to achieve 100% when it comes to implementing risk mitigating actions concerning cyber-security threats. However, as a starting point, it was considered appropriate to pitch the acceptable responses to just over the 50% mark.

This section contains the results of the cyber-security status of the metropolitan municipalities that participated in the study. The demographic profile of the sample is discussed first, followed by the frequencies per question. The reliability of subscales is reported on next, followed by descriptive statistics per subscale. Differences in knowledge and attitudes between municipalities are reported using the one-way analysis of variance (ANOVA) and Chi-square test. Lastly, the relationship between demographic variables and the subscales is discussed. These were investigated using the one-way ANOVA and non-parametric correlations.

8.6.1. Demographic frequencies

The demographic profile of the sample is described below.

Tenure

There was a fairly even spread between the categories of tenure, with roughly 20% of respondents in each of the first three categories. A further 13.4% had between seven and ten years of service, while almost a quarter of the respondents (24.8%) had more than ten years of service. Overall, it appears to be quite an established workforce. Details are illustrated in the table and figure below.

Table 8.2: Tenure

		Frequency	Percent	Valid percent	Cumulative percent
Valid	<3 years	71	20.7	20.7	20.7
	3-5 years	71	20.7	20.7	41.4
	5-7 years	70	20.4	20.4	61.8
	7-10 years	46	13.4	13.4	75.2
	10+ years	85	24.8	24.8	100.0
	Total	343	100.0	100.0	

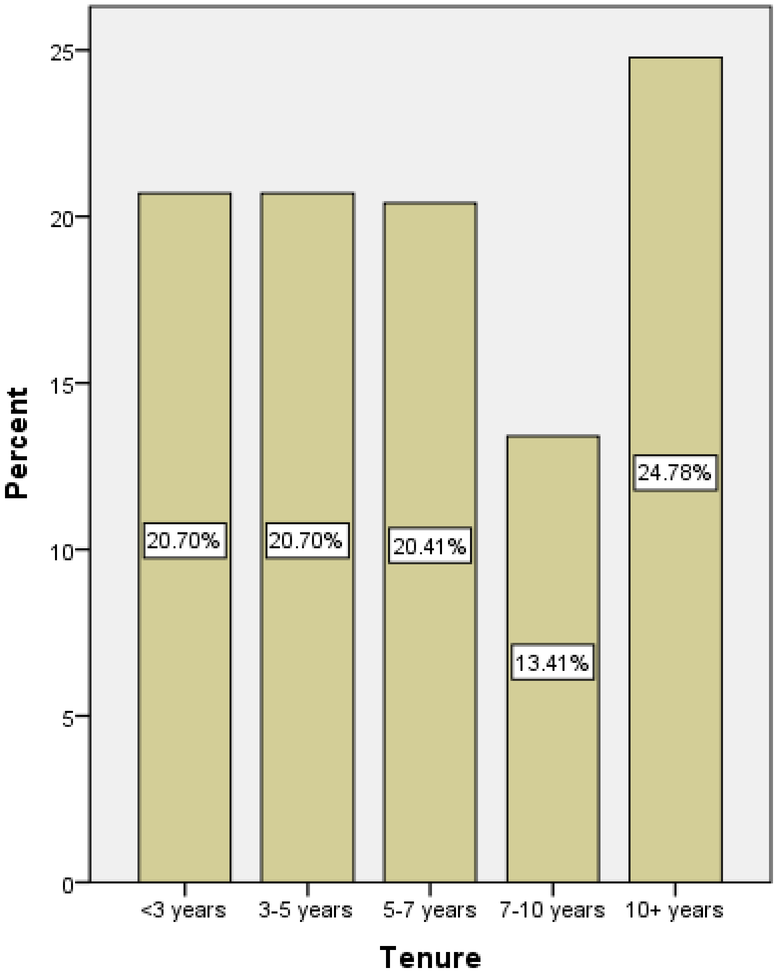


Figure 8.3: Tenure

Category

Respondents were represented in one of three work categories, with a fairly evenly spread between these, as listed in the table and figure below. Roughly a third of the group fell in each category.

Table 8.3: Category

		Frequency	Percent	Valid percent	Cumulative percent
Valid	Information and Communication	106	30.9	30.9	30.9
	Operating	112	32.7	32.7	63.6
	Administration	125	36.4	36.4	100.0
	Total	343	100.0	100.0	

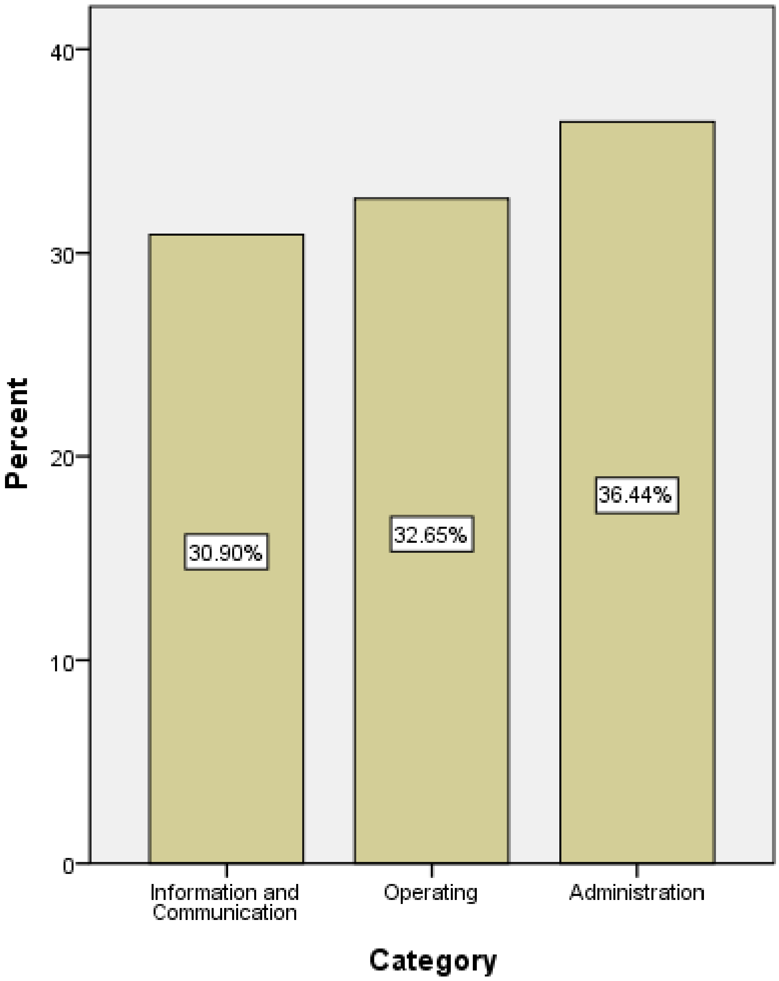


Figure 8.4: Category

Level

Just less than half of the respondents (46.4%) were at the specialist level. About one in every four respondents (25.4%) was at a clerical level, while the remainder (28.3%) formed part of management (see table and figure below).

Table 8.4: Level

		Frequency	Percent	Valid percent	Cumulative percent
Valid	Management	97	28.3	28.3	28.3
	Specialist	159	46.4	46.4	74.6
	Clerical	87	25.4	25.4	100.0
	Total	343	100.0	100.0	

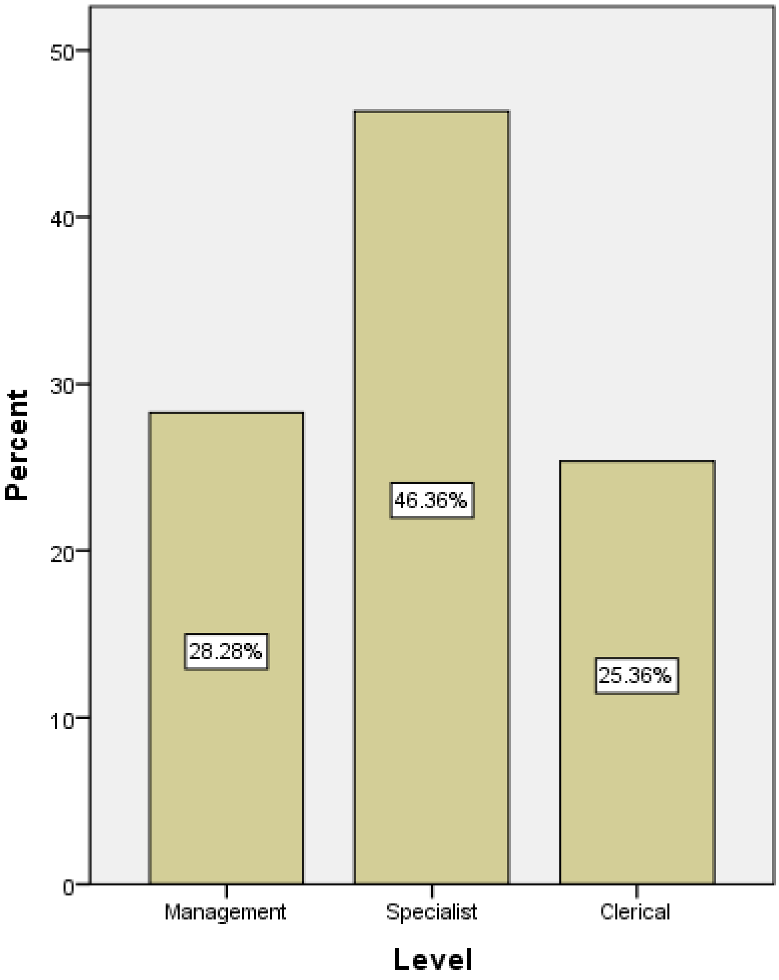


Figure 8.5: Level

Municipality

As shown in the table and figure below, in terms of Municipality, the largest single group (39.9%) was from Tshwane, while 33.2% were from NMBM. The smallest group of respondents (26.8%) were from Durban municipality.

Table 8.5: Municipality

		Frequency	Percent	Valid percent	Cumulative percent
Valid	Durban	92	26.8	26.8	26.8
	NMBM	114	33.2	33.2	60.1
	Tshwane	137	39.9	39.9	100.0
	Total	343	100.0	100.0	

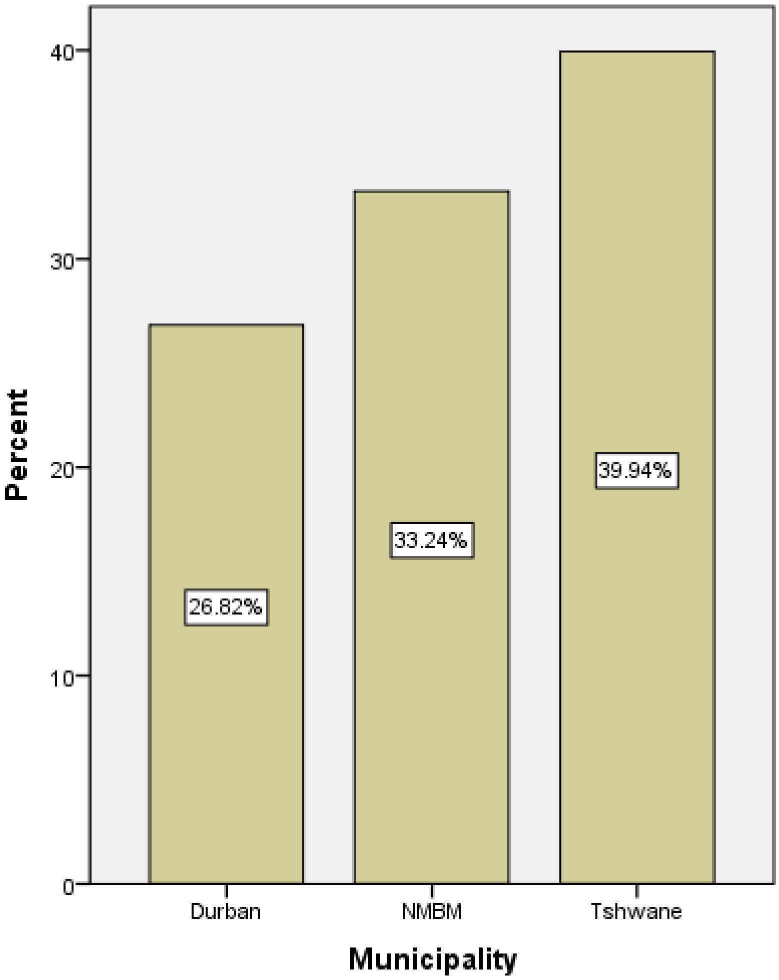


Figure 8.6: Municipality

8.6.2. Descriptive statistics per question

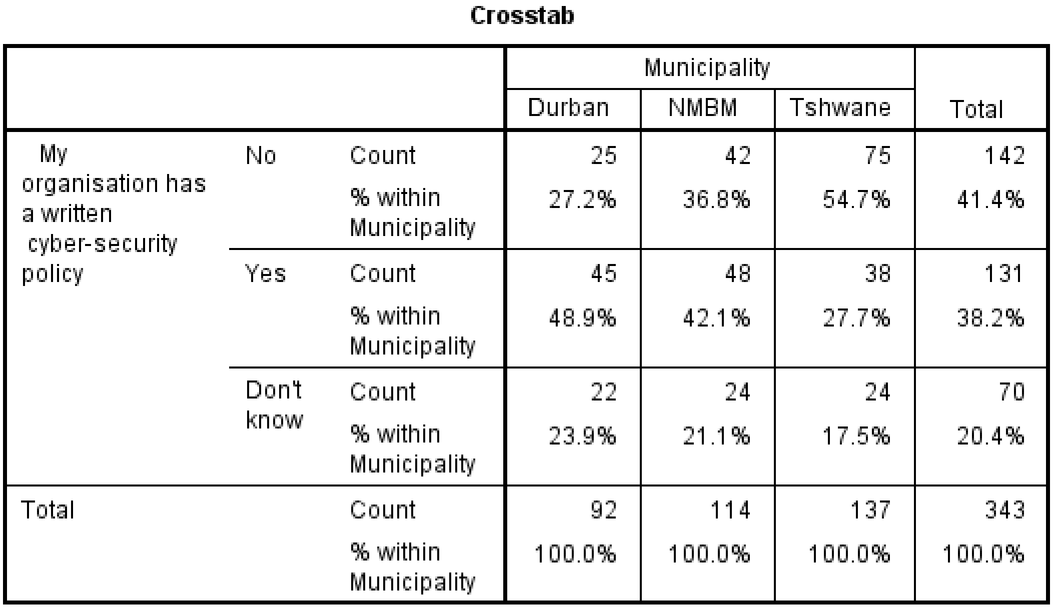
There were essentially two types of questions in the questionnaire. Some questions were primarily knowledge questions, which were answered using the options Yes, No and don't know. The remainder of the questions were more related to attitudes, and a 5-point scale from strongly agree to strongly disagree was used. The middle option was a "don't know" option. While this option is reflected in the frequencies, it was removed for the sake of calculating the mean score per item and constructing a scale. The descriptive statistics per item are reported for the knowledge questions first, and then for the attitude questions.

The "don't know" option was chosen by the participants in each question, and across the three pertinent municipalities. With the intention of creating a positive cyber-security culture in the organisation, the "don't know" response was considered a negative viewpoint. All employees in an organisation must know or have knowledge of applicable cyber-security risk mitigating controls. Overall 20.4% of respondents indicated they don't know if their organisation has a written cyber-security policy. The "don't know" response statistics in each question, per municipality, and across all the three municipalities are presented in the following sections.

8.6.2.1. Knowledge questions

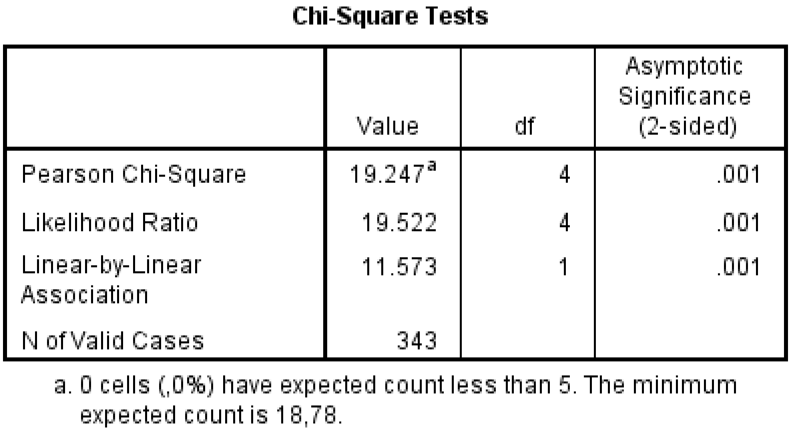
The frequencies per item for the knowledge questions are reported and briefly discussed below. Since it is possible that the *de facto* situation could differ from one municipality to the next, the results are presented per municipality. In each case, cross tabulations are presented and are followed by a Chi-square analysis and a figure (graph). These all indicate whether the differences between municipalities are significant.

Table 8.6: My organisation has a written cyber-security policy



Crosstab

			Municipality			Total
			Durban	NMBM	Tshwane	
My organisation has a written cyber-security policy	No	Count	25	42	75	142
		% within Municipality	27.2%	36.8%	54.7%	41.4%
	Yes	Count	45	48	38	131
		% within Municipality	48.9%	42.1%	27.7%	38.2%
	Don't know	Count	22	24	24	70
		% within Municipality	23.9%	21.1%	17.5%	20.4%
Total		Count	92	114	137	343
		% within Municipality	100.0%	100.0%	100.0%	100.0%



Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	19.247[a]	4	.001
Likelihood Ratio	19.522	4	.001
Linear-by-Linear Association	11.573	1	.001
N of Valid Cases	343		

a. 0 cells (,0%) have expected count less than 5. The minimum expected count is 18,78.

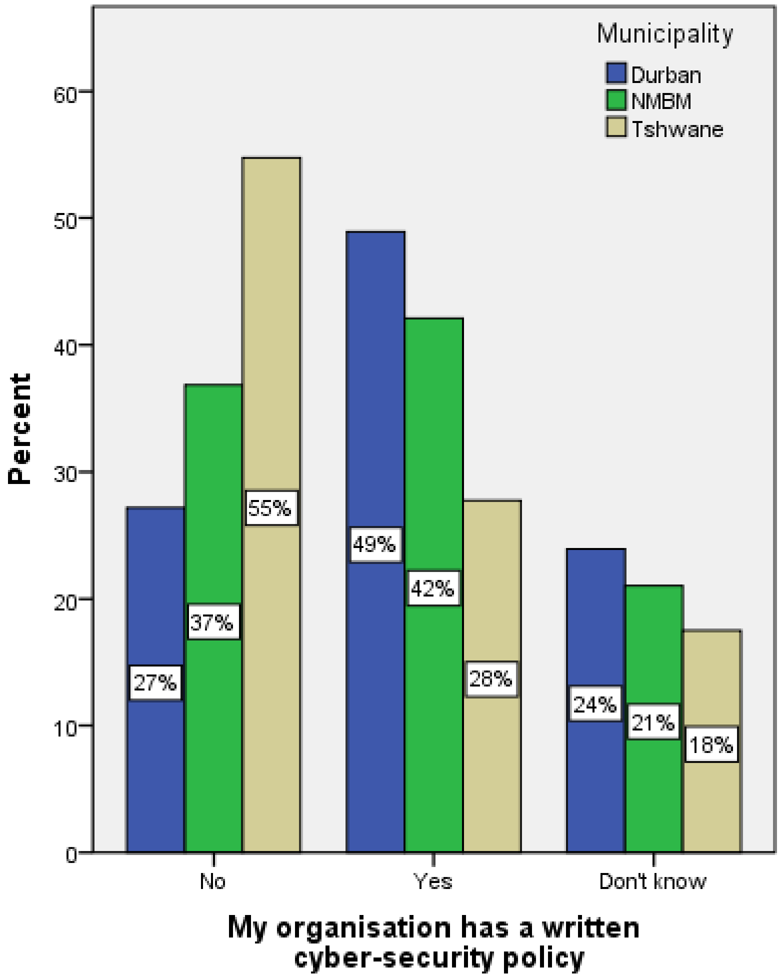
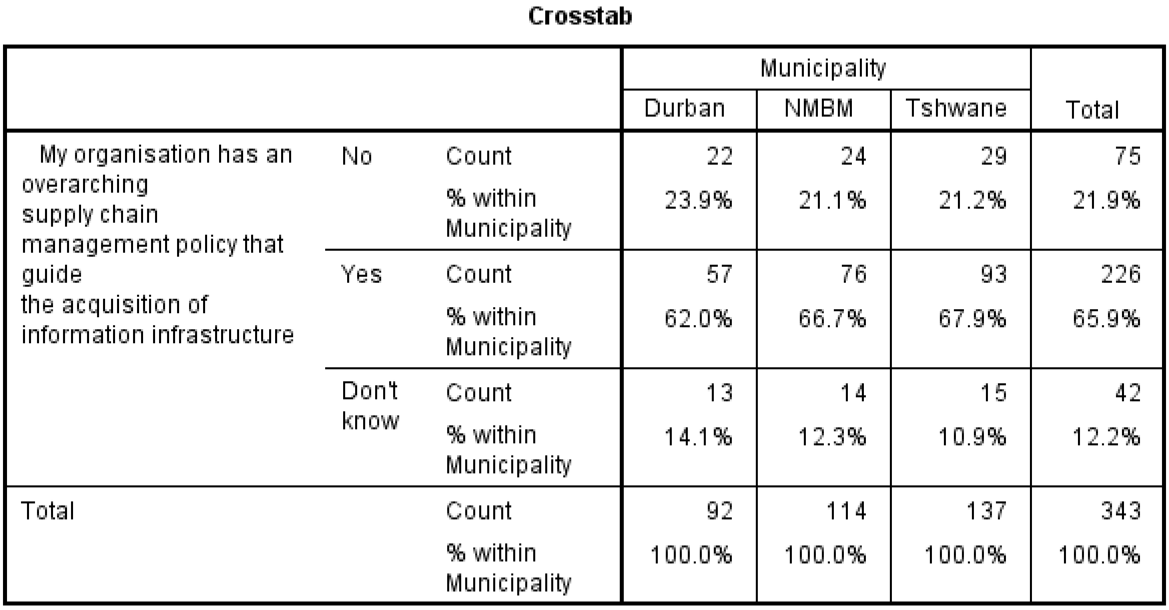


Figure 8.7: My organisation has written a cyber-security policy

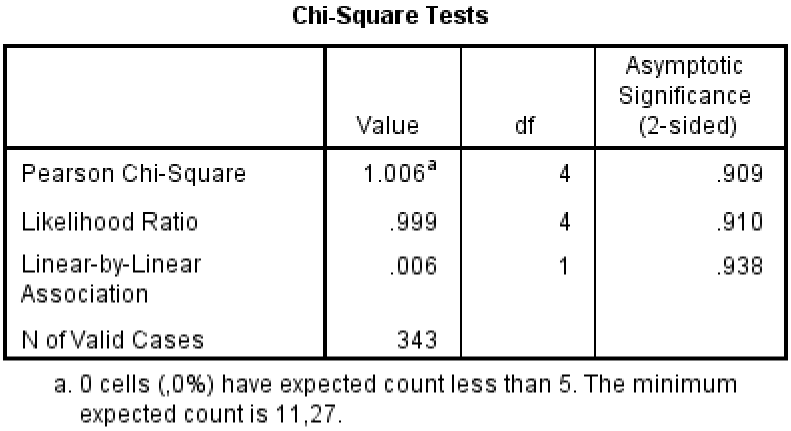
There was a significant difference between municipalities in terms of respondents' knowledge of a written cyber-security (p<0.05). Based on these cross-tabulations, it is clear that more than half of the Tshwane respondents (54.7%) indicated that they do not have a cyber-security policy in place. Almost the opposite was the case in Durban, where just under half of the respondents (48.9%) indicated that there is a policy in place. However, 23.9% of the respondents from Durban did not know whether there was a policy in place. The ignorance was less in Pretoria, where 17.5% of respondents were uncertain. In NMBM, 42.1% indicated that there is a policy in place, while 36.8% said that there is not. Overall, however, it would appear that there is not much clarity amongst municipal employees about this issue. Clearly, more work is required on the implementation of cyber-security policy throughout the municipalities.

Table 8.7: My organisation has an overarching supply chain management policy that guides the acquisition of information infrastructure



Crosstab

			Municipality			Total
			Durban	NMBM	Tshwane	
My organisation has an overarching supply chain management policy that guide the acquisition of information infrastructure	No	Count	22	24	29	75
		% within Municipality	23.9%	21.1%	21.2%	21.9%
	Yes	Count	57	76	93	226
		% within Municipality	62.0%	66.7%	67.9%	65.9%
	Don't know	Count	13	14	15	42
		% within Municipality	14.1%	12.3%	10.9%	12.2%
Total		Count	92	114	137	343
		% within Municipality	100.0%	100.0%	100.0%	100.0%



Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	1.006[a]	4	.909
Likelihood Ratio	.999	4	.910
Linear-by-Linear Association	.006	1	.938
N of Valid Cases	343		

a. 0 cells (,0%) have expected count less than 5. The minimum expected count is 11,27.

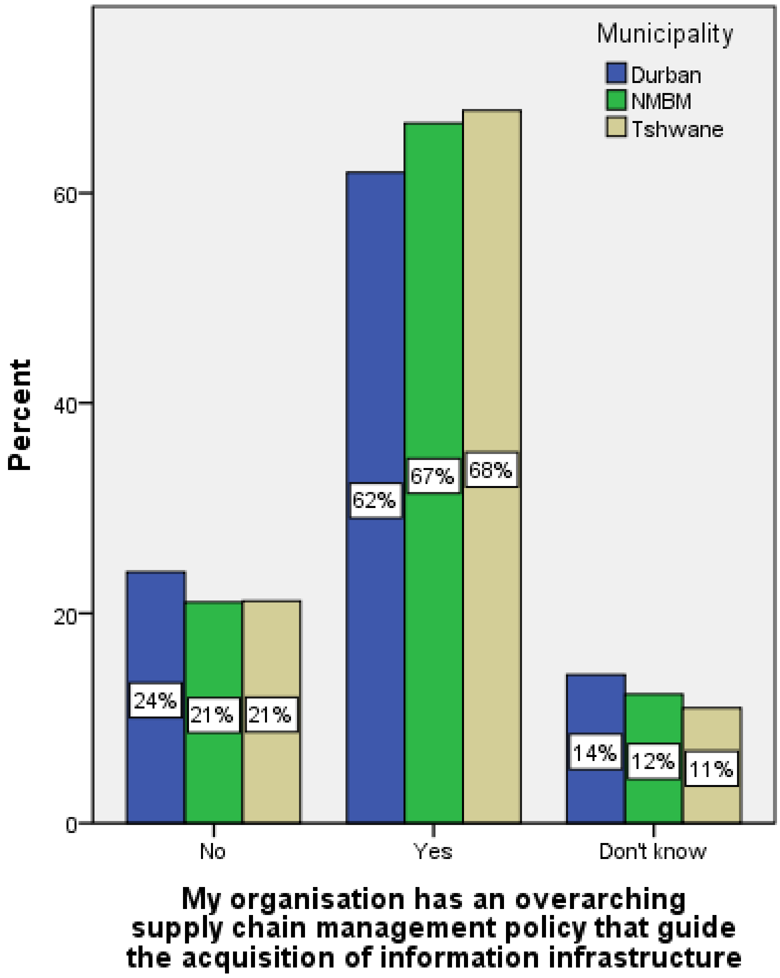
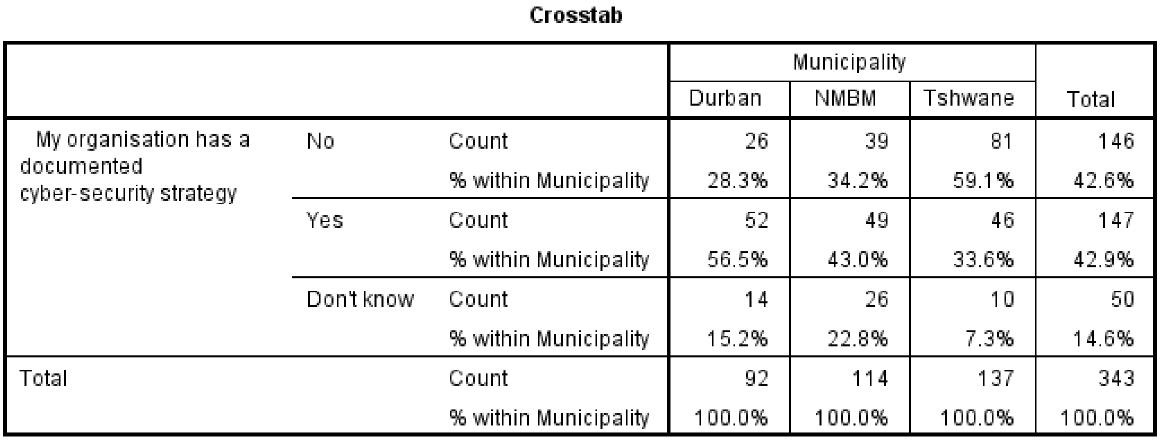


Figure 8.8: My organisation has an overarching supply chain management policy that guides the acquisition of information infrastructure

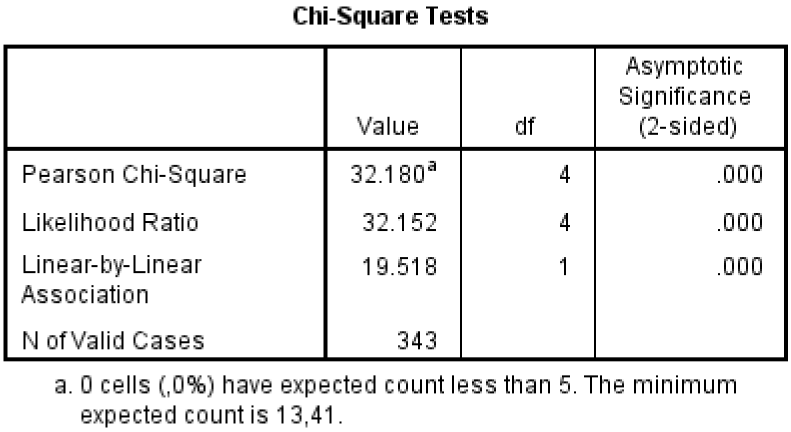
With regard to the overarching supply chain management policy, there were no significant differences between municipalities. Between 62.0% and 67.9% of respondents in all municipalities indicated that there is indeed a policy, while between 21.2% and 23.9% disagreed with the statement. The levels of uncertainty ranged from 10.9% to 14.1%.

Table 8.8: My organisation has a documented cyber-security strategy



Crosstab

			Municipality			Total
			Durban	NMBM	Tshwane	
My organisation has a documented cyber-security strategy	No	Count	26	39	81	146
		% within Municipality	28.3%	34.2%	59.1%	42.6%
	Yes	Count	52	49	46	147
		% within Municipality	56.5%	43.0%	33.6%	42.9%
	Don't know	Count	14	26	10	50
		% within Municipality	15.2%	22.8%	7.3%	14.6%
Total		Count	92	114	137	343
		% within Municipality	100.0%	100.0%	100.0%	100.0%



Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	32.180[a]	4	.000
Likelihood Ratio	32.152	4	.000
Linear-by-Linear Association	19.518	1	.000
N of Valid Cases	343		

a. 0 cells (,0%) have expected count less than 5. The minimum expected count is 13,41.

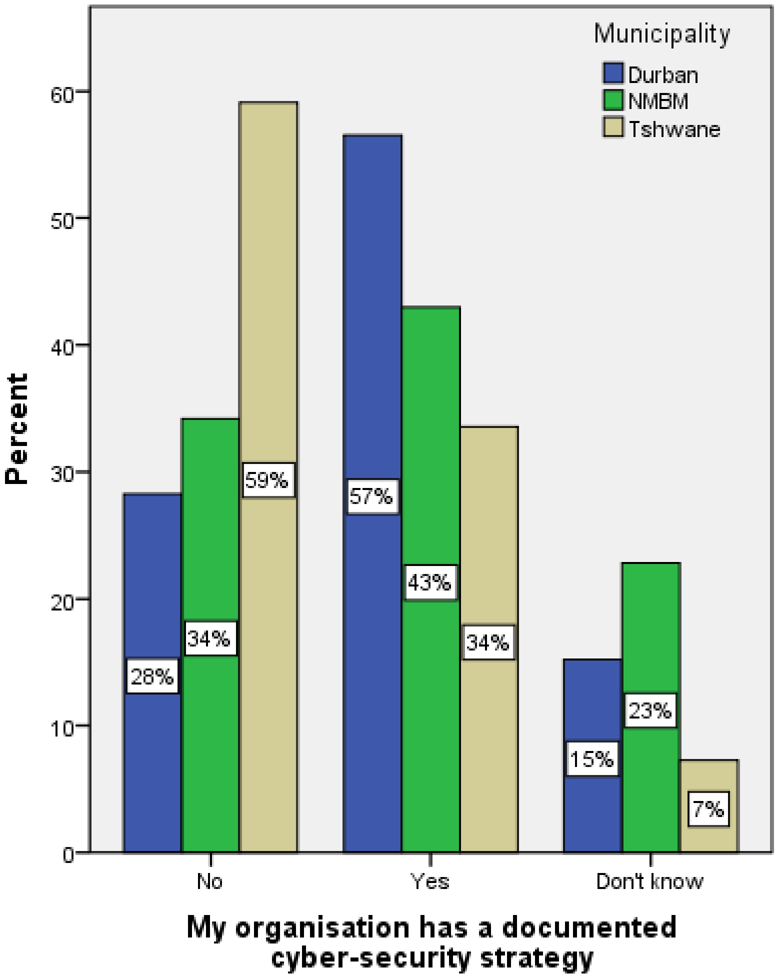
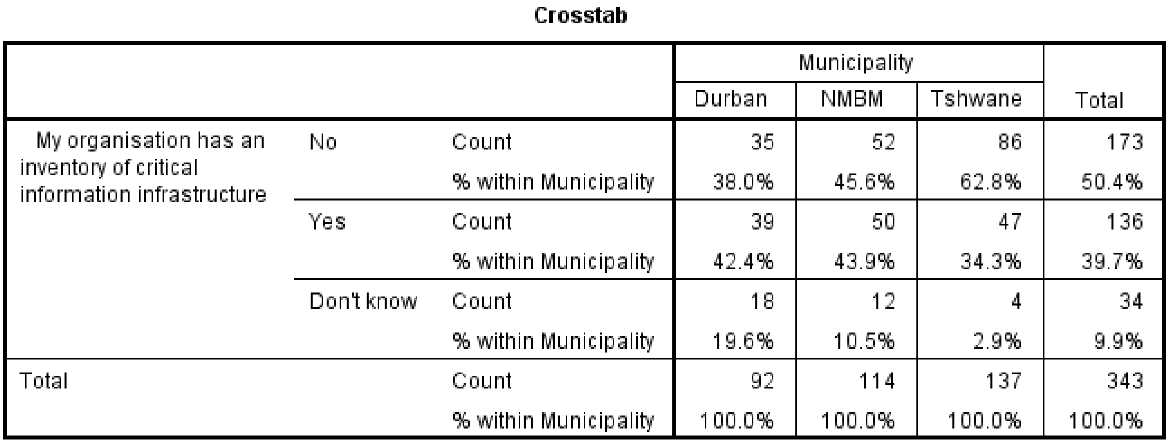


Figure 8.9: My organisation has a documented cyber-security strategy

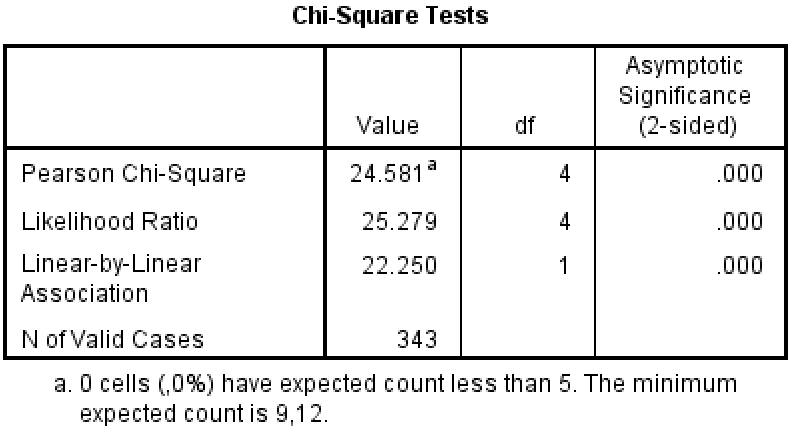
Municipalities differed significantly from one another with regard to this question. Patterns were similar to the first question, with 59.1% of respondents from Tshwane indicating that this is not the case, and 56.5% of respondents from Durban indicating that it is the case. In the case of NMBM, 34.2% of respondents answered affirmatively, and 43% in the negative. A total of 22.8% in this municipality were uncertain.

Table 8.9: My organisation has an inventory of critical information infrastructure



Crosstab

			Municipality			Total
			Durban	NMBM	Tshwane	
My organisation has an inventory of critical information infrastructure	No	Count	35	52	86	173
		% within Municipality	38.0%	45.6%	62.8%	50.4%
	Yes	Count	39	50	47	136
		% within Municipality	42.4%	43.9%	34.3%	39.7%
	Don't know	Count	18	12	4	34
		% within Municipality	19.6%	10.5%	2.9%	9.9%
Total		Count	92	114	137	343
		% within Municipality	100.0%	100.0%	100.0%	100.0%



Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	24.581[a]	4	.000
Likelihood Ratio	25.279	4	.000
Linear-by-Linear Association	22.250	1	.000
N of Valid Cases	343		

a. 0 cells (,0%) have expected count less than 5. The minimum expected count is 9,12.

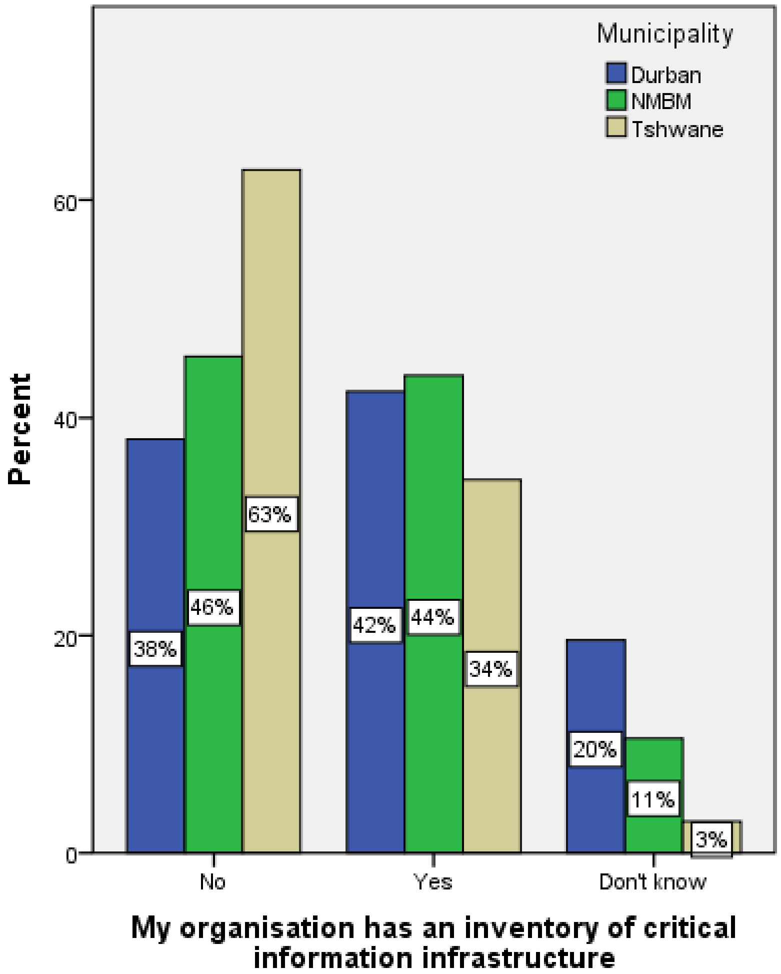
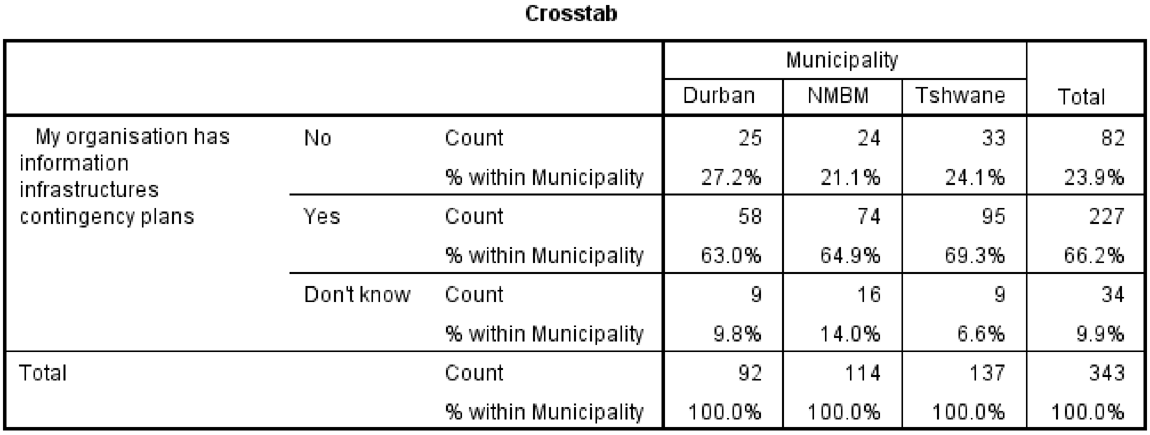


Figure 8.10: My organisation has an inventory of critical information infrastructure

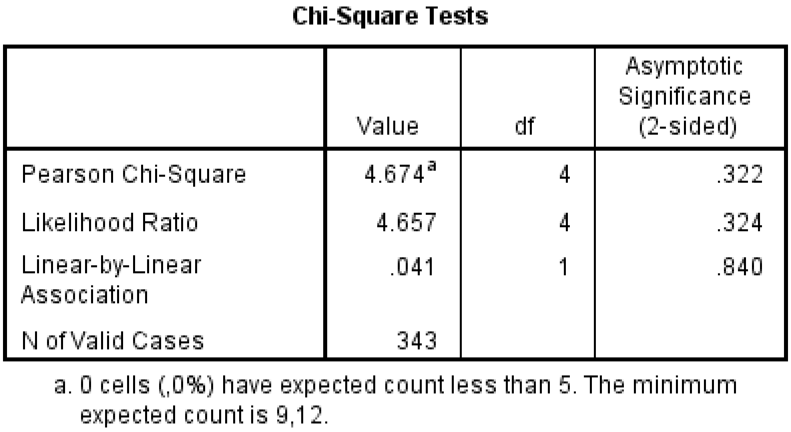
Responses to this question showed a significant pattern in relation to each municipality. In NMBM, almost equal percentages answered “yes” (43.9%) and “no” (45.6%) respectively. In Durban, opinions were also somewhat divided, with almost one in five respondents indicating that they did not know. The majority of respondents from Tshwane (62.8%), however, confirmed that such an inventory does not exist.

Table 8.10: My organisation has information infrastructure contingency plans



Crosstab

			Municipality			Total
			Durban	NMBM	Tshwane	
My organisation has information infrastructures contingency plans	No	Count	25	24	33	82
		% within Municipality	27.2%	21.1%	24.1%	23.9%
	Yes	Count	58	74	95	227
		% within Municipality	63.0%	64.9%	69.3%	66.2%
	Don't know	Count	9	16	9	34
		% within Municipality	9.8%	14.0%	6.6%	9.9%
Total		Count	92	114	137	343
		% within Municipality	100.0%	100.0%	100.0%	100.0%



Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	4.674[a]	4	.322
Likelihood Ratio	4.657	4	.324
Linear-by-Linear Association	.041	1	.840
N of Valid Cases	343		

a. 0 cells (,0%) have expected count less than 5. The minimum expected count is 9,12.

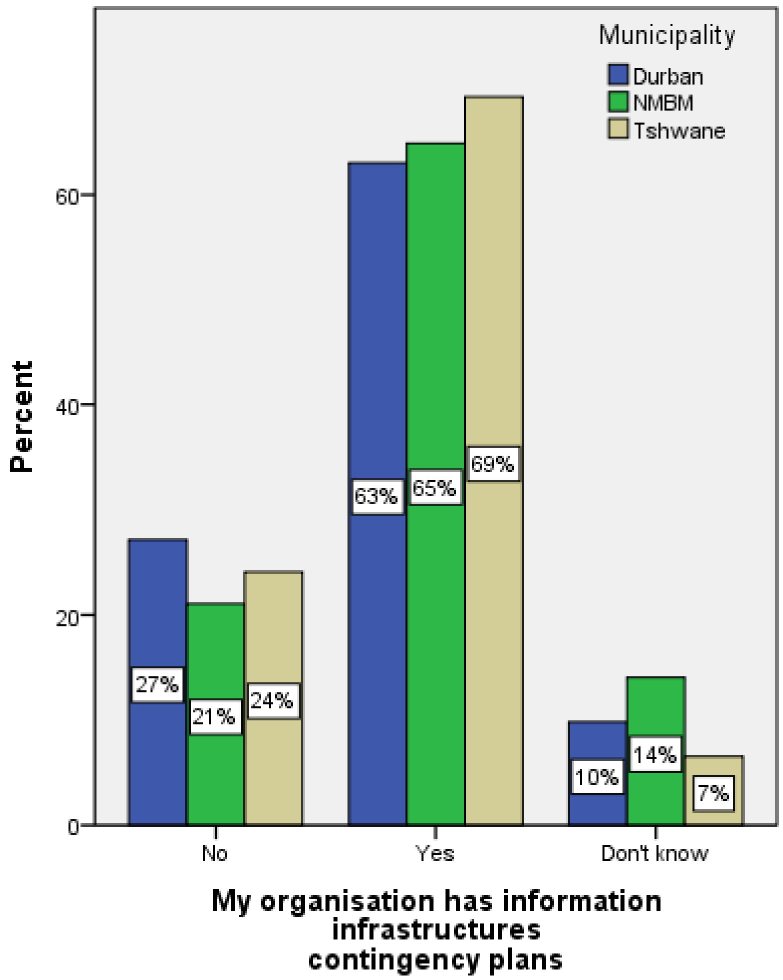
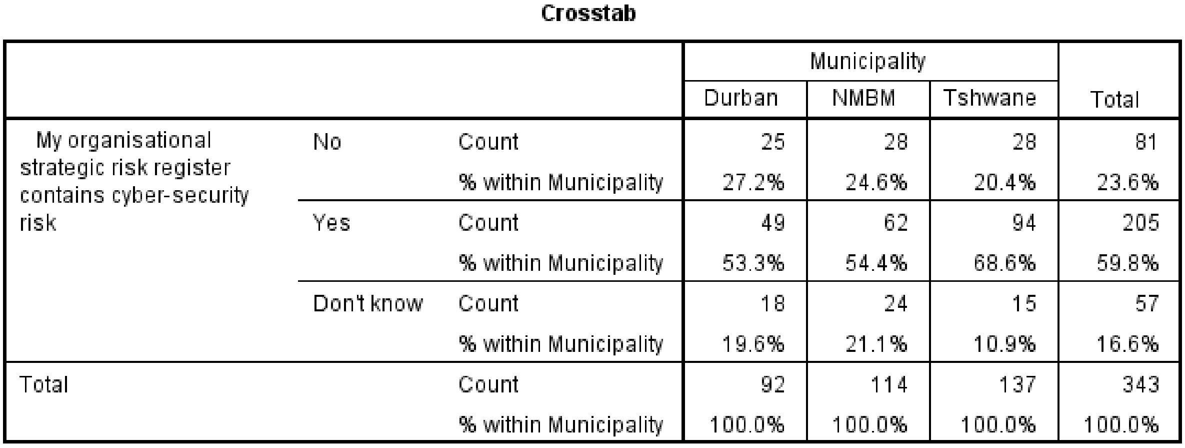


Figure 8.11: My organisation has information infrastructure contingency plans

With regard to contingency plans, there were no significant differences between the responses from the municipalities. In all municipalities, the majority of respondents indicated that such plans are indeed in place.

Table 8.11: My organisational strategic risk register contains cyber-security risk



Crosstab

			Municipality			Total
			Durban	NMBM	Tshwane	
My organisational strategic risk register contains cyber-security risk	No	Count	25	28	28	81
		% within Municipality	27.2%	24.6%	20.4%	23.6%
	Yes	Count	49	62	94	205
		% within Municipality	53.3%	54.4%	68.6%	59.8%
	Don't know	Count	18	24	15	57
		% within Municipality	19.6%	21.1%	10.9%	16.6%
Total		Count	92	114	137	343
		% within Municipality	100.0%	100.0%	100.0%	100.0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	8.599[a]	4	.072
Likelihood Ratio	8.798	4	.066
Linear-by-Linear Association	.091	1	.762
N of Valid Cases	343		

a. 0 cells (,0%) have expected count less than 5. The minimum expected count is 15,29.

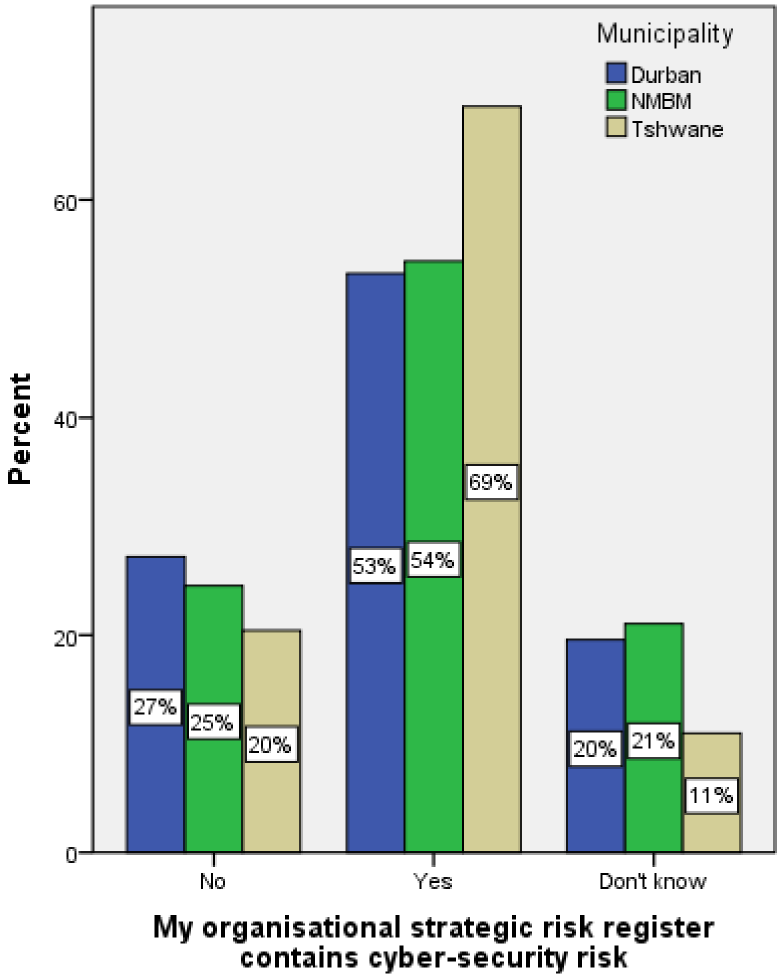
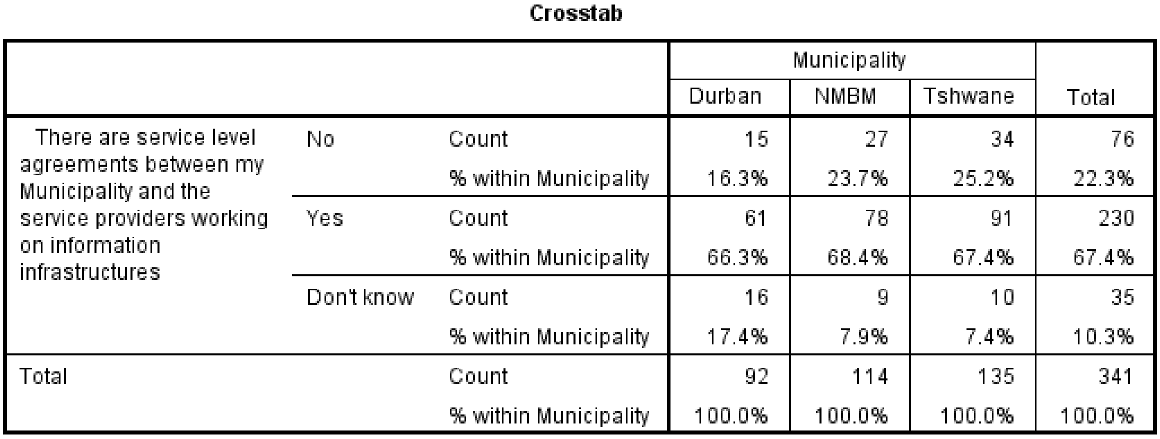


Figure 8.12: My organisational strategic risk register contains cyber-security risk

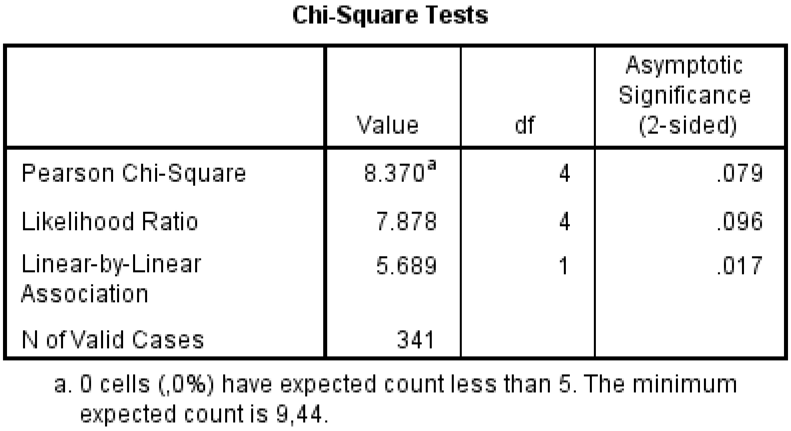
There were no statistically significant differences between municipalities concerning the strategic risk register. In Durban and NMBM, just over half of the respondents indicated that this is indeed the case, while 68.6% of respondents from Tshwane confirmed this.

Table 8.12: There are service level agreements between my municipality and the service providers working on information infrastructures



Crosstab

			Municipality			Total
			Durban	NMBM	Tshwane	
There are service level agreements between my Municipality and the service providers working on information infrastructures	No	Count	15	27	34	76
		% within Municipality	16.3%	23.7%	25.2%	22.3%
	Yes	Count	61	78	91	230
		% within Municipality	66.3%	68.4%	67.4%	67.4%
	Don't know	Count	16	9	10	35
		% within Municipality	17.4%	7.9%	7.4%	10.3%
Total		Count	92	114	135	341
		% within Municipality	100.0%	100.0%	100.0%	100.0%



Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	8.370[a]	4	.079
Likelihood Ratio	7.878	4	.096
Linear-by-Linear Association	5.689	1	.017
N of Valid Cases	341		

a. 0 cells (,0%) have expected count less than 5. The minimum expected count is 9,44.

There were no statistically significant differences between municipalities concerning service level agreements. In all three municipalities, around two thirds of respondents confirmed that this is in place. In Tshwane, one in four respondents indicated that this is not the case. In Durban, there was the largest degree of uncertainty (17.4%).

8.6.2.2. Attitude questions

Attitude questions were initially measured on a 5-point scale. For the sake of brevity, a summary is provided in Table 8.13 below, showing the frequencies and percentages per option, as well as the mean score per question. These results are for the sample as a whole.

Table 8.13: Summary of responses to the attitude questions

Item	Statistic	Response option					Mean
		Strongly disagree	Disagree	Agree	Strongly agree	Don't know	
The cyber-security policy contains sections that are relevant to my job	f	35	76	203	11	18	2,64
	%	10,20	22,16	59,18	3,21	5,25	
The cyber-security policy is aligned to the Municipal Integrated Development Plan (IDP)	f	21	95	191	0	36	2,58
	%	6,12	27,70	55,69	0,00	10,50	
I believe our Cyber-security strategy is aligned to the Municipal IDP	f	14	75	174	51	29	2,55
	%	4,08	21,87	50,73	14,87	8,45	
There is a structure or unit within my organisation that is responsible to implement the cyber-security strategy	f	20	75	157	53	38	2,83
	%	5,83	21,87	45,77	15,45	11,08	
I know what to do if I want to report breaches or violations against cyber-security policy	f	46	117	157	17	6	2,80
	%	13,41	34,11	45,77	4,96	1,75	
I know who the custodian of the cyber-security policy is	f	37	86	120	48	52	2,43
	%	10,79	25,07	34,99	13,99	15,16	
My organisation conducts research and development with the aim to enhance protection of information infrastructure	f	35	148	120	22	18	2,62
	%	10,20	43,15	34,99	6,41	5,25	
Protection of information infrastructure in my organisation is guided by the industry best practises	f	23	62	184	44	30	2,40
	%	6,71	18,08	53,64	12,83	8,75	
Management has allocated adequate budget to implement cyber-security policy	f	55	63	132	56	28	2,80
	%	16,03	18,37	38,48	16,33	8,16	
Risk Management processes guide the implementation of cyber-security controls in my organisation	f	36	57	163	62	25	2,54
	%	10,50	16,62	47,52	18,08	7,29	
Management has provided guidance on the regulatory requirements pertaining to information infrastructure that I work with	f	19	74	175	52	23	2,79
	%	5,54	21,57	51,02	15,16	6,71	
Management has allocated adequate people to protection information infrastructures	f	74	97	125	16	31	2,81
	%	21,57	28,28	36,44	4,66	9,04	
Management enforces compliance to cyber-security	f	27	67	145	62	42	2,27
	%	7,87	19,53	42,27	18,08	12,24	
In my organisation there are oversight structures / committees that make management to account for the protection of information infrastructure	f	30	97	137	42	37	2,80
	%	8,75	28,28	39,94	12,24	10,79	
Internal Audit operational plans incorporate audits or reviews on information infrastructures on an annual basis	f	29	90	175	29	20	2,62
	%	8,45	26,24	51,02	8,45	5,83	
Management have input in the Internal Audit operational plans before the plan is implemented	f	28	78	164	48	25	2,63
	%	8,16	22,74	47,81	13,99	7,29	
Audit Committee approves the internal audit operational plans before the plan is implemented	f	46	73	135	62	27	2,73
	%	13,41	21,28	39,36	18,08	7,87	
Management has implemented clear asset management practices	f	33	66	154	44	46	2,67
	%	9,62	19,24	44,90	12,83	13,41	
Management understands the possible impact of cyber-security threats to Municipal service delivery	f	42	61	151	43	46	2,70
	%	12,24	17,78	44,02	12,54	13,41	
Management is monitoring the services provided by the service providers / consultants against the service level agreements	f	35	44	189	48	27	2,66
	%	10,20	12,83	55,10	13,99	7,87	
My organisation has deployed technologies to protect information infrastructures against cyber threats	f	39	48	151	77	28	2,79
	%	11,37	13,99	44,02	22,45	8,16	
Access to information infrastructures is controlled through identification and authentication	f	39	52	166	53	33	2,84
	%	11,37	15,16	48,40	15,45	9,62	
Management has adopted industry best practises to protect information infrastructure against cyber-threats	f	25	55	176	59	28	2,75
	%	7,29	16,03	51,31	17,20	8,16	
Anti-virus software are installed into our laptops, desktops, and other devices	f	33	76	90	104	40	2,85
	%	9,62	22,16	26,24	30,32	11,66	
Audits are conducted to provide assurance on the adequacy and effectiveness of controls that have been implemented to protect information infrastructure	f	46	95	128	40	34	2,87
	%	13,41	27,70	37,32	11,66	9,91	
The incident management procedures are adequate to resolve cyber-security incidents	f	48	86	103	76	30	2,52
	%	13,99	25,07	30,03	22,16	8,75	
The building that I work in is adequately protected to secure the information infrastructure	f	47	75	154	47	20	2,66
	%	13,70	21,87	44,90	13,70	5,83	
Employees’ activities on information infrastructure are monitored	f	42	82	159	37	23	2,62
	%	12,24	23,91	46,36	10,79	6,71	
In my organisation action is taken against employees who violate cyber-security policy	f	61	38	159	51	34	2,60
	%	17,78	11,08	46,36	14,87	9,91	
Employees are made aware of the cyber-security policy contents	f	15	129	135	34	30	2,65
	%	4,37	37,61	39,36	9,91	8,75	
Employees know where to report suspicious illicit cyber-security activities	f	72	73	134	48	16	2,60
	%	20,99	21,28	39,07	13,99	4,66	
Employees receive adequate training on the information infrastructure they operate	f	32	74	160	60	17	2,48
	%	9,33	21,57	46,65	17,49	4,96	
I am aware of cyber-security threats affecting the information assets I work with	f	51	70	136	59	27	2,76
	%	14,87	20,41	39,65	17,20	7,87	
I am aware that organisational Internet and e-mail systems should be used for business purposes	f	43	58	150	68	24	2,64
	%	12,54	16,91	43,73	19,83	7,00	
Employees accept responsibility towards information infrastructure protection	f	40	76	163	30	34	2,59
	%	11,66	22,16	47,52	8,75	9,91	
My organisation constantly conducts cyber-security assessment to determine how employees are complying with the cyber-security policy	f	72	142	74	13	42	2,09
	%	20,99	41,40	21,57	3,79	12,24	

Inspection of the table above shows that opinion was relatively divided for most questions, leading to mean scores which all lie in the mid-range of the scale, with a slight slant towards the positive side. It is possible that differences between municipalities can account for the moderate spread, with some municipalities being more inclined to agree and others more inclined to disagree. For this reason, a one-way ANOVA was conducted on the item scores to compare municipalities.

The questions for which there were significant differences are summarised below. Descriptive statistics per group are also reported. For the sake of brevity, only questions which reached a significance level of 0.01 are reported.

Table 8.14: Questions with significance level 0.01 and post hoc results

Item	Sig F	Post hoc result
The cyber-security policy is constantly reviewed to incorporate emerging trends in the protection of information infrastructures	0,005	Durban significantly higher than both Tshwane and NMBM
Management enforces compliance to cyber-security	0,001	Durban significantly higher than Tshwane
Audit Committee approves the internal audit operational plans before the plan is implemented	0,006	Durban significantly higher than both Tshwane and NMBM
Management has implemented clear asset management practices	0,001	Durban significantly higher than both Tshwane and NMBM
In my organisation action is taken against employees who violate cyber-security policy	0,003	Durban significantly higher than both Tshwane and NMBM

Table 8.15: Descriptives

		N	Mean	Std. Deviation
The cyber-security policy is constantly reviewed to incorporate emerging trends in the protection of information infrastructures	Durban	84	2.88	.701
	NMBM	106	2.58	.893
	Tshwane	134	2.54	.732
	Total	324	2.64	.792
Management enforces compliance to cyber-security	Durban	79	3.05	.766
	NMBM	101	2.85	.921
	Tshwane	121	2.60	.841
	Total	301	2.80	.867
Audit committee approves the internal audit operational plans before the plan is implemented	Durban	85	2.95	.937
	NMBM	107	2.59	1.009
	Tshwane	124	2.56	.877

	Total	316	2.67	.952
Management has implemented clear asset management practices	Durban	74	3.00	.682
	NMBM	100	2.54	.937
	Tshwane	123	2.66	.838
	Total	297	2.70	.854
In my organisation, action is taken against employees who violate cyber-security policy	Durban	82	2.96	.922
	NMBM	104	2.55	1.042
	Tshwane	123	2.52	.917
	Total	309	2.65	.978
I am aware of cyber-security threats affecting the information assets I work with	Durban	83	2.93	.894
	NMBM	107	2.54	.984
	Tshwane	126	2.54	.960
	Total	316	2.64	.964

There is a clear pattern for the Durban municipality which has higher scores (more positive attitude) than the other two municipalities. Tshwane and NMBM do not differ significantly from one another.

8.6.3. Reliability

The questionnaire was intended to measure attitudes towards four domains of cybersecurity, namely:

- integrated development
- governance
- technical operations
- human issues.

The reliability of these scales was investigated by means of a Cronbach alpha in order to establish whether they show internal consistency and can thus be used as scales. Reliability statistics are summarised below.

Table 8.16: Reliability statistics

Scale	Cronbach's alpha	Average inter-item correlation
Integrated development	0,361	0,067
Governance	0,817	0,295
Technical operations	0,713	0,232
Human issues	0,743	0,233

According to Bryman and Bell (2007, p. 164), Cronbach alpha values of 0.70 and above are typically employed as a rule of thumb to denote a good level of internal reliability, while Clark and Watson (1995) suggested that the average inter-item correlation of items should be between 0.1 and 0,5.

Using these guidelines, results showed that the first scale did not show adequate reliability. Inspection of the questions revealed that this may be due to questions which pertain more to knowledge being included as attitude questions. The remainder of the scales were found to possess adequate internal consistency, and were used in subsequent analyses.

8.6.4. Descriptive statistics per subscale

Mean scores per subscale were calculated and are reported below. Mean scores could theoretically range from 1 (Strongly disagree) to 4 (Strongly agree). (The don't know option was removed for the sake of scale construction as it is not equal to a "neutral" attitude). A higher mean score is thus associated with a more positive attitude towards the particular aspect.

It is clear from the table and graph below that the mean scores on the three scales are very similar, and range from 2.57 – 2.74. On the 4-point scale, this falls just above the midpoint of the scale (2.5). Overall it would appear that respondents had fairly moderate opinions towards these aspects, with a very slight tendency towards the more positive side of the scale. Further nuances will most probably appear when delving deeper into subgroup differences.

Table 8.17: Descriptive statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Governance domain	343	1.45	3.82	2.6564	.44765
Technical operations domain	343	1.50	3.75	2.7431	.51199
Human issues	343	1.22	3.63	2.5792	.48357
Valid N (listwise)	343				

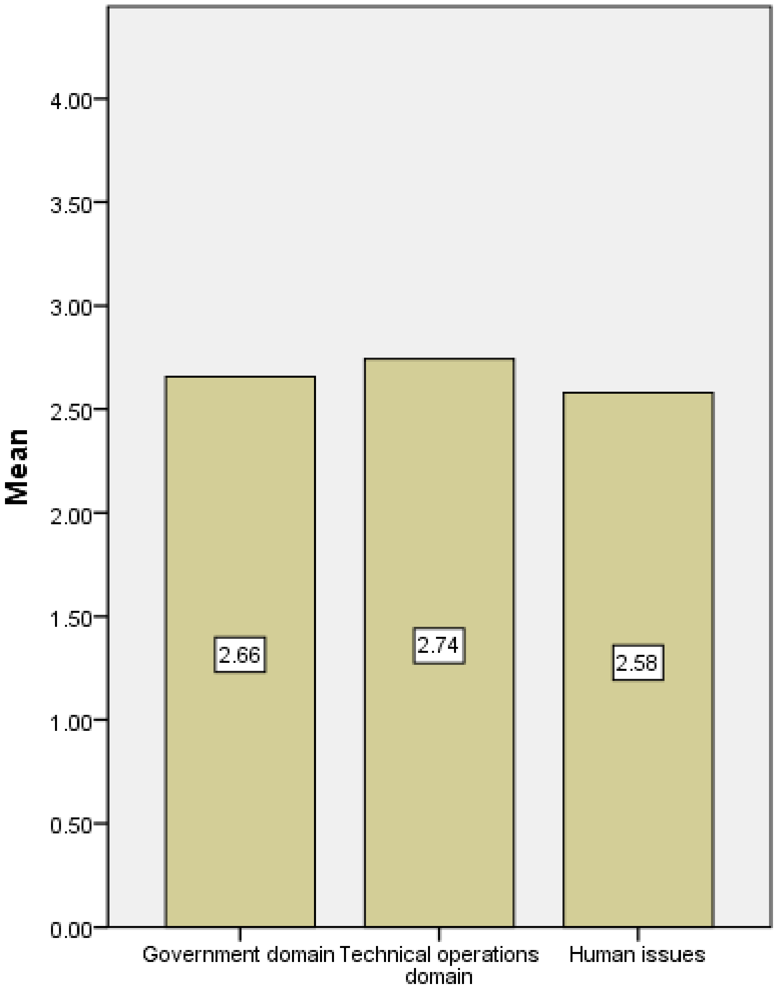


Figure 8.13: Descriptive statistics

8.6.5. Comparison of municipalities

One of the objectives of this study was to investigate the differences in perceptions between municipalities. A one-way ANOVA was performed in order to investigate mean differences between the municipalities on the three subscales. The 5% level of significance was used. Results are reported below.

Table 8.18: Descriptives

		N	Mean	Std. Deviation	Std. Error
Governance domain	Durban	92	2.8002	.43734	.04560
	NMBM	114	2.6191	.49691	.04654
	Tshwane	137	2.5908	.38897	.03323
	Total	343	2.6564	.44765	.02417
Technical operations domain	Durban	92	2.9051	.49365	.05147
	NMBM	114	2.7462	.50739	.04752
	Tshwane	137	2.6318	.50196	.04288
	Total	343	2.7431	.51199	.02764
Human issues	Durban	92	2.7430	.38988	.04065
	NMBM	114	2.5003	.52916	.04956
	Tshwane	137	2.5348	.47784	.04083
	Total	343	2.5792	.48357	.02611

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Government domain	Between Groups	2.649	2	1.325	6.836	.001
	Within Groups	65.883	340	.194		
	Total	68.532	342			
Technical operations domain	Between Groups	4.115	2	2.057	8.178	.000
	Within Groups	85.533	340	.252		
	Total	89.648	342			
Human issues	Between Groups	3.447	2	1.723	7.656	.001
	Within Groups	76.527	340	.225		
	Total	79.974	342			

The ANOVA table above shows that there are significant mean differences between the municipalities on all three scales (p<0.05). The nature of these differences were investigated further by means of post hoc tests.

Table 8.19: Multiple comparisons
Scheffe

Dependent variable	(I) Municipality	(J) Municipality	Mean Difference (I-J)	Std. Error	Sig.
Government domain	Durban	NMBM	.18104*	.06169	.014
		Tshwane	.20936*	.05933	.002
	NMBM	Durban	-.18104*	.06169	.014
		Tshwane	.02832	.05580	.879
	Tshwane	Durban	-.20936*	.05933	.002
		NMBM	-.02832	.05580	.879
Technical operations domain	Durban	NMBM	.15896	.07029	.079
		Tshwane	.27337*	.06761	.000
	NMBM	Durban	-.15896	.07029	.079
		Tshwane	.11441	.06358	.200
	Tshwane	Durban	-.27337*	.06761	.000
		NMBM	-.11441	.06358	.200
Human issues	Durban	NMBM	.24262*	.06649	.001
		Tshwane	.20819*	.06395	.005
	NMBM	Durban	-.24262*	.06649	.001
		Tshwane	-.03443	.06014	.849
	Tshwane	Durban	-.20819*	.06395	.005
		NMBM	.03443	.06014	.849

*. The mean difference is significant at the 0.05 level.

With regard to the governance domain, post hoc tests show that there was a significant difference between Durban and NMBM (p=0.014), as well as between Durban and Tshwane (p=0.002). There was not a significant difference between NMBM and Tshwane (p=0.879). Inspection of the mean scores show that Durban municipality had a higher scores than the other two municipalities (i.e. a more positive attitude).

Regarding the Technical operations, the only significant difference was found between Durban and Tshwane (p=0.000). Durban had the higher mean score of the 2. None of the other pairwise differences were significant.

Lastly, on Human issues, the same pattern as in the case of the government domain was found. There was a significant difference between Durban and NMBM (p=0.001), as well as between Durban and Tshwane (p=0.005). There was not a significant difference between NMBM and Tshwane (p=0.849). Once again, Durban had a higher score than the other two entities. The graphical presentation below illustrates the nature of these differences.

It should be kept mind that all scores still fall within a fairly small range from one another, and are just slightly higher than the midpoint of the scale. Nevertheless, it does appear that employees from Durban have a slightly more positive attitude towards the aspects measured.

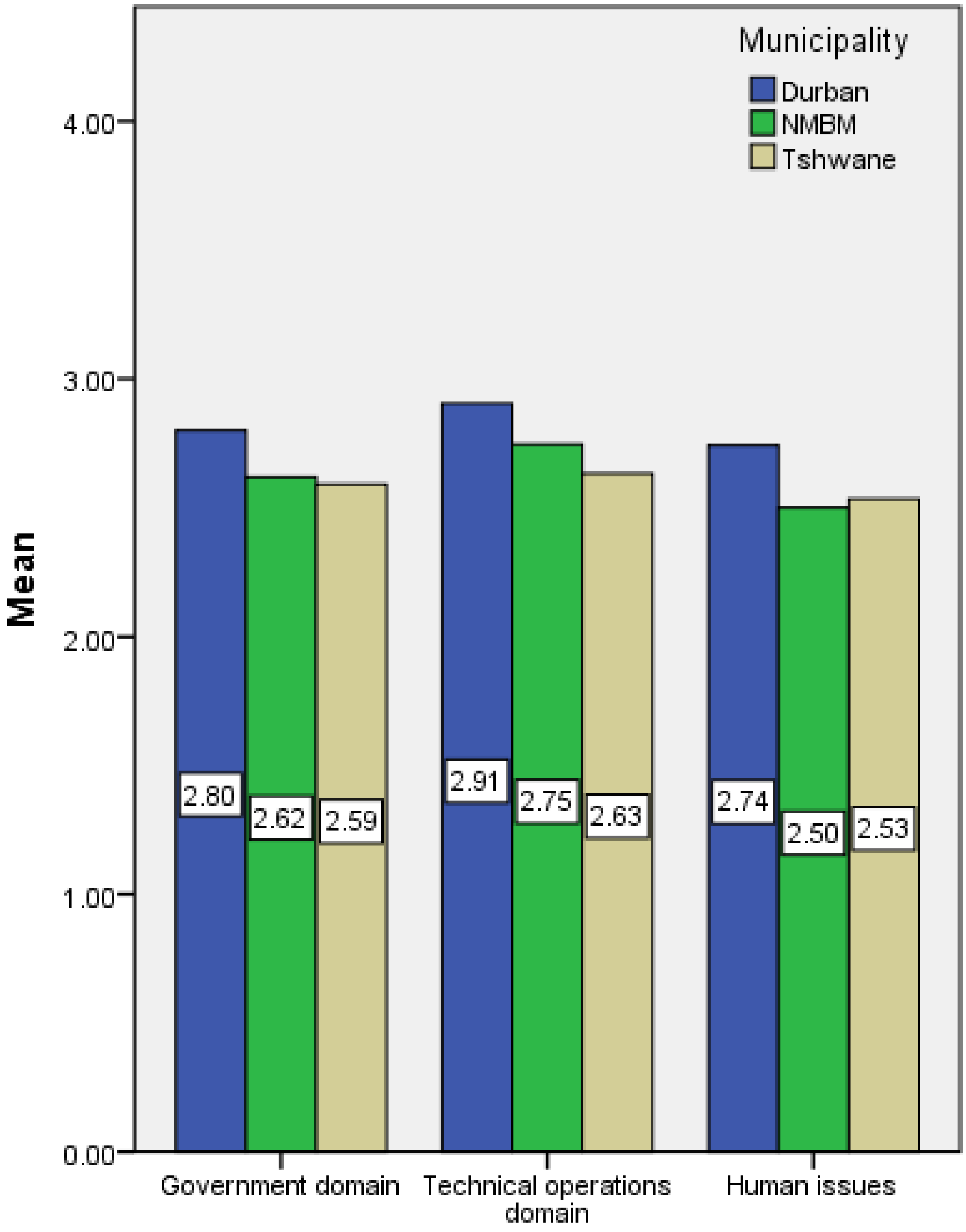


Figure 8.14: Multiple comparisons

8.6.6. Relationship between demographic variables and subscales

The relationship between demographic variables and the subscales was investigated by means of a one-way ANOVA. Results are reported below. Note that post hoc tests are only reported for those scales where significant overall differences were found.

Level

Respondents represented management, specialist and clerical levels. Their scores are compared below.

Table 8.20: Descriptives

		N	Mean	Std. Deviation	Std. Error
Government domain	Management	97	2.5710	.42851	.04351
	Specialist	159	2.7423	.43639	.03461
	Clerical	87	2.5944	.46507	.04986
	Total	343	2.6564	.44765	.02417
Technical operations domain	Management	97	2.6070	.40594	.04122
	Specialist	159	2.8964	.50722	.04023
	Clerical	87	2.6147	.55207	.05919
	Total	343	2.7431	.51199	.02764
Human issues	Management	97	2.5723	.45627	.04633
	Specialist	159	2.6264	.49254	.03906
	Clerical	87	2.5005	.49134	.05268
	Total	343	2.5792	.48357	.02611

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Government domain	Between Groups	2.215	2	1.107	5.677	.004
	Within Groups	66.318	340	.195		
	Total	68.532	342			
Technical operations domain	Between Groups	6.968	2	3.484	14.327	.000
	Within Groups	82.680	340	.243		
	Total	89.648	342			
Human issues	Between Groups	.897	2	.448	1.928	.147
	Within Groups	79.077	340	.233		
	Total	79.974	342			

From the ANOVA table it appears that the levels differed significantly with regard to their perceptions of the governance domain and technical operations ($p<0.05$). No significant differences were found with regard to Human Issues ($p>0.05$). Further investigation by means of post hoc tests show that, with regard to the Government domain, the only significant difference was between management and specialist staff, with the latter showing a significantly higher mean score than the former.

In the technical operations domain, specialists showed a significantly higher score than both management and clerical staff.

It would thus appear that, with regard to the governance domain, specialists tended to have slightly more positive attitudes than management staff. In terms of technical operations, specialists were slightly more positive than both management and clerical staff.

Table 8.21: Multiple comparisons

Scheffe

Dependent variable	(I) Level	(J) Level	Mean difference (I-J)	Std. Error	Sig.
Government domain	Management	Specialist	-.17127*	.05690	.011
		Clerical	-.02339	.06521	.938
	Specialist	Management	.17127*	.05690	.011
		Clerical	.14789*	.05890	.044
	Clerical	Management	.02339	.06521	.938
		Specialist	-.14789*	.05890	.044
Technical operations domain	Management	Specialist	-.28938*	.06353	.000
		Clerical	-.00765	.07282	.994
	Specialist	Management	.28938*	.06353	.000
		Clerical	.28173*	.06576	.000
	Clerical	Management	.00765	.07282	.994
		Specialist	-.28173*	.06576	.000

*. The mean difference is significant at the 0.05 level.

Results are portrayed graphically below.

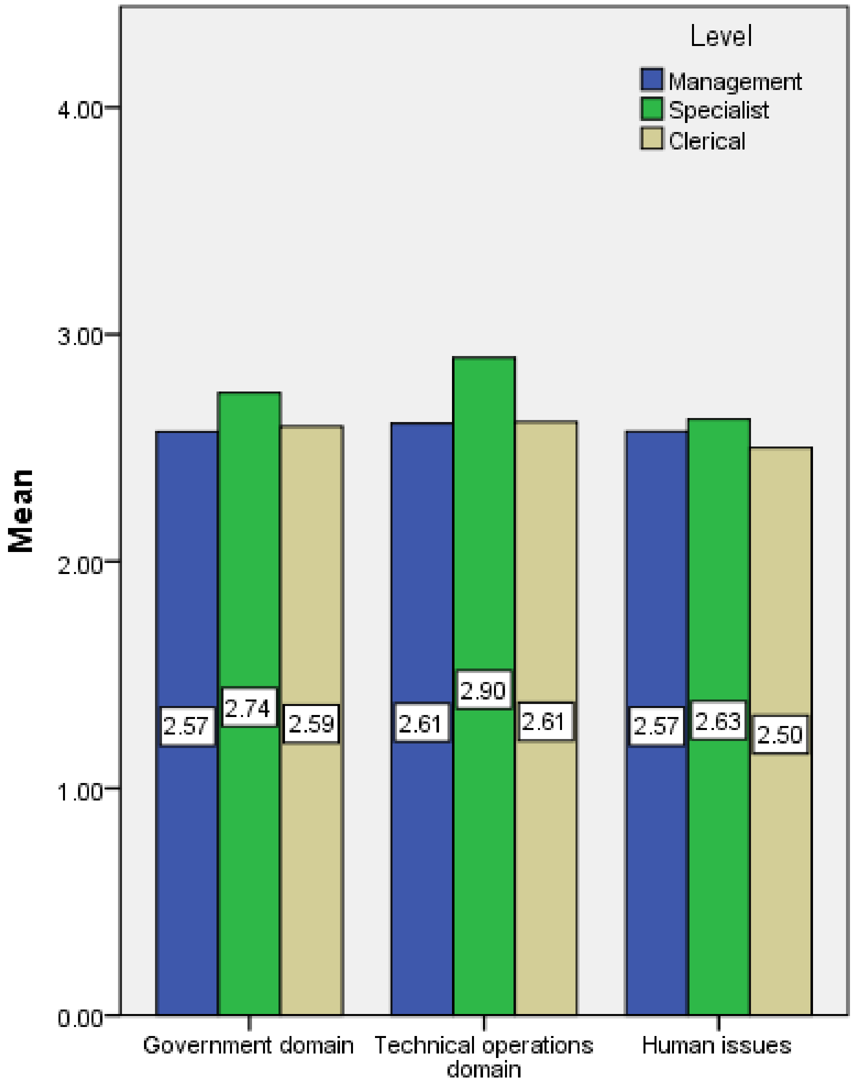


Figure 8.15: Multiple comparisons

Category

Respondents came predominantly from three categories, namely Information and communication, Operating, and Administration. The comparison of these groups by means of a one-way ANOVA is reported below.

Table 8.22: Descriptives

		N	Mean	Std. Deviation	Std. Error
Government domain	Information and Communication	106	2.6630	.55366	.05378
	Operating	112	2.7210	.31418	.02969
	Administration	125	2.5928	.44369	.03969
	Total	343	2.6564	.44765	.02417
Technical operations domain	Information and Communication	106	2.7751	.54676	.05311
	Operating	112	2.9789	.38767	.03663
	Administration	125	2.5048	.47637	.04261
	Total	343	2.7431	.51199	.02764
Human issues	Information and Communication	106	2.4817	.56774	.05514
	Operating	112	2.7559	.31803	.03005
	Administration	125	2.5035	.48923	.04376
	Total	343	2.5792	.48357	.02611

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Government domain	Between Groups	.978	2	.489	2.460	.087
	Within Groups	67.554	340	.199		
	Total	68.532	342			
Technical operations domain	Between Groups	13.438	2	6.719	29.976	.000
	Within Groups	76.210	340	.224		
	Total	89.648	342			
Human issues	Between Groups	5.224	2	2.612	11.880	.000
	Within Groups	74.750	340	.220		
	Total	79.974	342			

The ANOVA table shows that there were significant differences between the categories with regard to Technical operations ($p < 0.05$) and Human issues ($p<0.05$). These differences were explored further by means of post hoc tests.

Table 8.23: Multiple comparisons

Scheffe

Dependent variable	(I) Category	(J) Category	Mean difference (I-J)	Std. Error	Sig.
Technical operations domain	Information and Communication	Operating	-.20387*	.06416	.007
		Administration	.27030*	.06251	.000
	Operating	Information and Communication	.20387*	.06416	.007
		Administration	.47417*	.06160	.000
	Administration	Information and Communication	-.27030*	.06251	.000
		Operating	-.47417*	.06160	.000
Human issues	Information and Communication	Operating	-.27428*	.06354	.000
		Administration	-.02182	.06191	.940
	Operating	Information and Communication	.27428*	.06354	.000
		Administration	.25246*	.06101	.000
	Administration	Information and Communication	.02182	.06191	.940
		Operating	-.25246*	.06101	.000

*. The mean difference is significant at the 0.05 level.

The post hoc tests show that, with regard to the technical operations domain there were significant differences between all three categories. Inspection of the mean scores reveals that respondents in the Operating category had the highest mean followed by those from Information and Communication. Administration had the lowest mean of the groups.

As far as human issues were concerned, the Operating category differed significantly from both the Information and communication ($p<0.05$) and Administration ($p<0.05$) categories. The latter two categories did not differ from one another though. Respondents in the Operating category had a significantly higher mean score than those in Administration, and Information and Communication Technology.

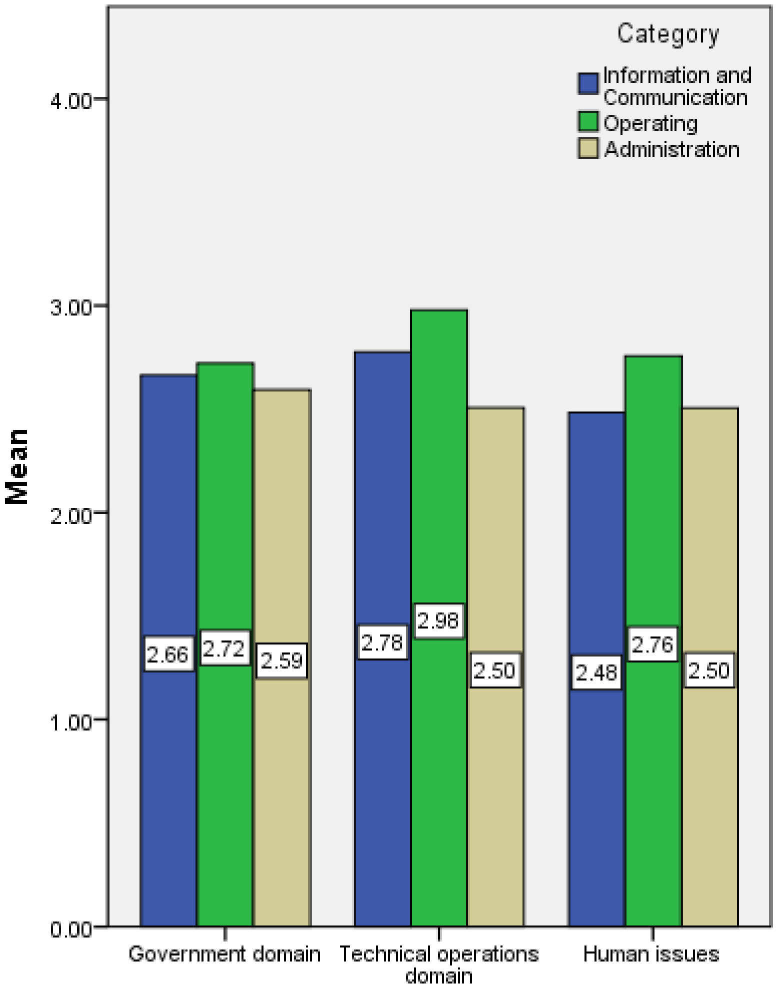


Figure 8.16: Multiple comparisons

Tenure

Tenure was measured in terms of five categories as indicated in the demographic frequency results. As such, it was treated as an ordinal variable, and a non-parametric Spearman's rho correlation was calculated between tenure and the subscales. Results are reported below and show that tenure showed statistically significant correlations with the Government domain ($p<0.05$) and Technical operations domain ($p<0.05$) scores. A correlation of -0.180 was found with the Government domain, suggesting a small negative association between the two variables. An even smaller correlation of -0,150 was found with the technical operations domain. Both suggest that the longer respondents were with the municipality, the more negative their perceptions were, but the trend is objectively very small. This is illustrated in the graph, where all mean values can be rounded off to 3.

Table 8.24: Correlations

		Tenure
Government domain	Pearson Correlation	-.180
	Sig. (2-tailed)	.001
	N	343
Technical operations domain	Pearson Correlation	-.150
	Sig. (2-tailed)	.005
	N	343
Human issues	Pearson Correlation	-.079
	Sig. (2-tailed)	.145
	N	343

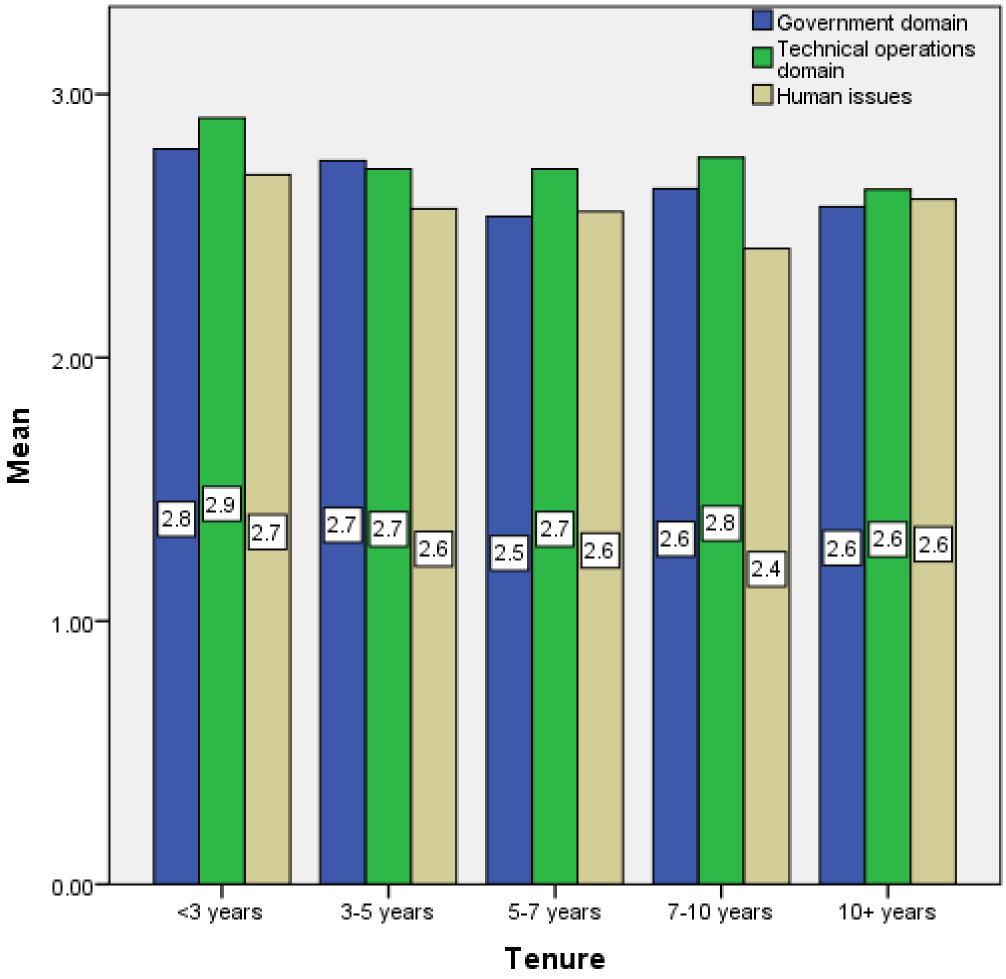


Figure 8.17: Correlations

8.7. CHAPTER SUMMARY

In this chapter, the results of the study were presented. The demographic profile of the sample was discussed, followed by descriptive statistics per question. Municipalities were also compared per question. The reliability of subscales was reported, followed by descriptive statistics per subscale. Differences in knowledge and attitudes between municipalities were investigated and the relationship between demographic variables and the subscales was reported on.

CHAPTER 9
CONCLUSION

9.1. CHAPTER INTRODUCTION

The principal research question that this study endeavoured to address is: What is the cyber-security status in South African metropolitan municipalities? This chapter revisits the research question and presents solutions for the research question. The study sub-questions are also revisited and solutions presented. The researcher contribution, study limitations, and future research are discussed.

9.2. REVISITING THE RESEARCH QUESTION

In order to answer the fundamental research question, the researcher formulated the following five sub-questions, which then assisted to explore various situations with the aim of providing the solution to the research question. The researcher first answered each sub-question before answering the core question. The following are the sub-questions together with solutions for each.

a. **How are metropolitan municipalities in South Africa protecting their information infrastructures against cyber-security threats?**

The researcher used ConGTM at eThekwini Metropolitan Municipality to explore how information infrastructures are protected against cyber-security threats. The grounded theory study resulted in a framework that indicated what activities are conducted to protect the information infrastructure against cyber-threats. The framework highlighted that four domains are at the centre of cyber-security in the municipality. These domains are integrated development cyber-security, cyber-security governance, cyber-security technical operations, and human issues in cyber-security.

The integrated development cyber-security is the core category which coordinates activities within each category. As the core category, the integrated development cyber-security category ensures that the following activities take place: development of cyber-security policy, procurement of information infrastructure is aligned with supply chain management policy, development of cyber-security strategy, formulation of critical information infrastructure catalogue, formulation of information infrastructure contingency plans, continuous reviewing and aligning the cyber-security policy to the municipal IDP, monitoring compliance to the cyber-security policy, conducting research and development on cyber-security, and introducing and sustaining the adoption of cyber-security industry best practices. The activities in the integrated development cyber-security domain are the responsibility of a designated cyber-security structure or function

The activities of the cyber-security governance category are a responsibility of executive management in the municipality. Cyber-security governance activities include: formulating a strategic risk register that includes cyber-security risk; formulating a regulatory and legislation framework that impacts on information infrastructure; allocating resources for cyber-security; setting the tone at the top by enforcing compliance to cyber-security policy, related regulation and legislation; implementing cyber-security oversight committees; implementing an internal audit programme to audit cyber-security controls; and driving the implementation of asset management practices.

The cyber-security technical operations category deals with ensuring that automated tools and people are deployed to implement the cyber-security policy. The activities in this category are mainly executed within various business units. The activities performed include: implementing and monitoring the service level agreements; deploying appropriate technologies to detect cyber threats; monitoring computer network activities; preventing unauthorised access to the computer network system (these technologies include anti-virus software, intrusion detection systems, intrusion prevention systems); implementing user identification and authentication mechanisms; adopting industry best practices on cyber-security; conducting audits and compliance testing on cyber-security; preparing and testing information infrastructure contingency procedures; and physically protecting the information infrastructure.

Human issues in cyber-security deal with ensuring that the first line of cyber-security defence, which comprises human beings, is addressed separately from other cyber-security activities. Cyber-security in the organisation is as good as people who are implementing it. The cyber-security human issues category has activities which include monitoring individual activities on information infrastructures; taking appropriate actions against individuals who violate the cyber-security policy; educating individual employees on the contents of the cyber-security policy and for employees to acknowledge understanding of the cyber-security policy; making employees aware where to report suspicious illicit activities on information infrastructure; training individual employees on the information infrastructure that they operate; educating users on the acceptable use of municipal internet and e-mail systems; and continuously assessing the cyber-security status in order to ensure that individual employees take responsibility for safeguarding the municipal information infrastructure.

The study objective for this sub-question was to explore the practices that metropolitan municipalities in South Africa have implemented to protect their information infrastructures against cyber-security threats. The ConGTM study as presented in Part I, specifically in Chapter 4, was conducted to achieve this research objective.

b. What methodologies are currently available to assess the cyber-security status in the metropolitan municipalities in South Africa?

Cyber-security assessment is conducted with the aim to cultivate cyber-security, and subsequently the protection of information infrastructure assets. Due to the infancy level of cyber-security in the country, there has been no known tools or methodologies that have been adopted to assess the cyber-security status in the South African metropolitan municipalities. Various studies have been conducted on cyber-security in the country; however, none has been designed to address the assessment of cyber-security status in metropolitan municipalities.

It has been highlighted that metropolitan municipalities in the country are largely dependent on information infrastructures. The grounded theory study has revealed that certain activities are performed to protect the information infrastructure against the cyber threats, and also that assurance services are conducted to assure management whether the cyber-security controls that they have been implemented are adequate and effective. Industry best practices have been adopted to safeguard municipal information infrastructures.

No tool has been tested to comprehensively assess the cyber-security posture of a metropolitan municipality. However, the grounded theory study has highlighted a number of controls that have been implemented to secure information infrastructure against cyber threats. These controls include: adoption of industry best practices such as the King IV report on corporate governance and Cobit, risk management processes, oversight by the audit committee, assurance by the office of the Auditor General of South Africa, cyber-security policy, management monitoring reports, information infrastructure acquisition, cyber-security sponsorship, asset management, user awareness and education, service level agreements, computer network monitoring, network vulnerability assessment, network protection (intrusion detection, intrusion prevention, and anti-virus software), user identification and authentication, compliance testing, asset disposal, contingency planning, performance management, segregation of duties, conduct of research and development, defence in depth, change management, and physical security of information infrastructure. Adoption of these controls has been audited but in a siloed fashion, thereby not proving a comprehensive view of the cyber-security status in the municipality. Assessing cyber-security requires a holistic/comprehensive view of the cyber-security controls that have been implemented to mitigate cyber-related risks.

Internal audit is one of the controls that have been implemented to advance the securing of information infrastructures in the municipalities. Assessing the status of cyber-security in the municipality requires considering to evaluate all the essential controls. Therefore, internal audit reports on their own do not provide conclusive reports on the status of cyber-security. This study therefore combined all the cyber-security-related controls, and grouped them into four domains and discussed them when answering sub-question (a) above. These controls assisted in developing the cyber-security assessment tool that was used to assess the cyber-security status in the three metropolitan municipalities, as discussed in Part II of this enquiry.

For this sub-question, the researcher wanted to explore the methodologies currently employed to assess the cyber-security status in the metropolitan municipalities in South Africa. The enquiry sought to discover the practices that metropolitan municipalities currently have adopted with the intention of assessing the cyber-security status. The reasons for assessing the status of cyber-security posture include:

(i) understanding the "as is" situation in order to draft the road map of getting into the desired destination to successfully protect the information infrastructure assets;
(ii) changing or enhancing the existing culture of cyber-security within the institution;
(iii) maintaining the current practices employed to protect information infrastructure against cyber-threats.

The practices that the study has uncovered are relevant in addressing the intentions of assessing the posture of cyber-security in the municipality.

c. How are metropolitan municipalities in South Africa inculcating the culture of cyber-security?

Cyber-security culture is one of the important components that provides and sustains an enabling environment for the protection of information infrastructure assets. The grounded theory study that was performed in this study also assisted in addressing this sub-question. The cyber-security controls that were highlighted by the participants indicate that a culture of cyber-security can be inculcated at various levels which are executive level, business unit level, and individual level. The research has highlighted that the executive level drives corporate governance within the municipality. Executive level management sets the tone for all other layers in pursuit of the municipal mandate. The employees that are participating on the executive layer are custodians of the municipal IDP processes. At the executive level, cyber-security culture in the municipality is mainly influenced by the way things are done at a strategic level in the municipality. The controls that are implemented at cyber-security governance domain of the municipal cyber-security framework are the ones that inculcate the culture of cyber-security. The cyber-security governance domain drives the implementation of an integrated development cyber-security domain, which is the essential domain that drives the cyber-security programme in the municipality. There is a cyclic relationship between the cyber-security governance domain and the integrated development cyber-security domain. The integrated development domain is responsible for co-ordinating and facilitating the activities of the cyber-security programme, which in turn must be sponsored at the executive level.

At business unit level, cyber-security is influenced by the controls that are executed by both the integrated development cyber-security domain and the cyber-security technical operations domain of the municipal cyber-security framework. The integrated development cyber-security domain prevents the siloed treatment of the cyber-security. The integrated development domain combines the ICT and PCS categories, and combines the efforts of all the units within the municipality that operate these categories. Technical implementation of automated tools and technologies to protect information infrastructure was also identified as an area that has an influence on the culture of cyber-security in the municipality. Technology and related tools are deployed and programmed, and they perform consistently as per the set configurations. Therefore, employees are forced to apply and comply as per the information infrastructure configurations. The cyber-security technical operations domain sets and maintains the security requirements as per the security policy and hence the inculcation of the cyber-security culture. At business unit level, the cyber-security culture is mainly influenced by the nature of the business/operations that the unit conducts, the nature of information infrastructure being operated (employees in a business unit are influenced by nature of monitoring and auditing in the unit), and the nature of leadership of the various business units to guide business units to comply with municipal policies and in making the right decisions about cyber-security.

At an individual level, the cyber-security culture is influenced by how cyber-security human issues are considered. Research participants indicated that the cyber-security controls in this domain include user training, ethical behaviour and attitude towards cyber-security, change management and cyber-security awareness.

The cyber-security assessment instrument that this study developed incorporates the culture element of cyber-security in the municipality. There is no specific domain that is called cyber-security culture, but all the four domains address the culture of cyber-security. The rating level of each item that is assessed in the assessment instrument indicates the level of cyber-security culture in that specific line item within a domain. When the control is rated as good that translates to good cyber-security culture; likewise, when the control rating is unsatisfactory, that translates to unsatisfactory cyber-security culture.

The researcher wanted to understand the processes that are employed to provide an enabling environment to develop, implement, and sustain a cyber-security culture in a metropolitan municipality. Identifying the processes employed to make the environment conducive for the information infrastructure protection is important to drive the agenda of cyber-security in the municipality.

d. What theoretical framework supports cyber-security implementation in the metropolitan municipalities in South Africa?

Part I of the study was designed to answer this question. One aspect of the ConGTM is to develop a theory. Due to the criticality of cyber-security, the researcher considered it imperative to seek explanations about cyber-security implementation in the metropolitan municipalities. The researcher wanted to determine what metropolitan municipalities do to implement cyber-security, and why do they do what they do to safeguard the information infrastructures against cyber risks.

The ConGTM study concluded with the formulation of the municipal cyber-security framework. The municipal cyber-security framework highlighted that there are four core categories that are considered when implementing cyber-security in the metropolitan municipality environment. These core categories are the following:

- Integrated development cyber-security which is the glue holding together all other categories. Mainly, this category is responsible for facilitating and coordinating the activities of the cyber-security programme within the municipality. This category is the gateway to communicating with other spheres of government such as the Department of Telecommunications and Postal Services which is responsible for the Cyber-security Hub in the country. The integrated development cyber-security category amongst other activities is responsible for cyber-security policy development, cyber-security strategy formulation, formulating an inventory of critical information infrastructure (these are more susceptible to cyber threats), and spearheading the cyber-security research and development within the municipality. The key role players in this domain are the people with specialist skills in the safeguarding of information assets/information infrastructure. This is the designated structure or function responsible for driving the functioning of the cyber-security programme in the municipality
- Cyber-security governance is responsible for setting the cyber-security tone in the municipality through sponsoring the cyber-security programme. The amount of budget allocation to fulfil information infrastructure protection determines the commitment of executive management to cyber-security. The core activities executed in the category include: setting up of the oversight structures that hold management to account for the cyber-security control deficiencies, approving cyber-security policy and strategy, formulating the applicable regulatory and legislation framework that the cyber-security programme must consider, and setting the asset management and supply chain management policies that the cyber-security programme must also consider. The role players in the category are the executive management team who are the custodians of municipal IDP processes.
- Cyber-security technical operations is responsible for commissioning the deployment of automated tools and technologies to secure information infrastructure. Activities of this category are conducted at a business unit level. Activities executed are geared

towards specific business units; however, these activities are guided by the type and nature of information infrastructure being operated in the unit/department. Business units are responsible for their departmental mission, vision, and objectives. Therefore, various business units are responsible for ensuring that the support that they receive from information infrastructures is maintained and enhanced. Business units are responsible for implementing the controls in pursuit of business unit objectives. It is therefore the business units' responsibility to implement and monitor the cyber-security controls that support the business unit to achieve its objectives.

- Cyber-security human issues are responsible for the social component of cyber-security and the focus is on an individual level in the organisation. Cyber-security technologies and tools can be implemented to secure information infrastructures, but without human beings to operate such technologies, those technologies can be rendered useless. Human issues in cyber-security mainly pay attention to the needs of the individual employees in order to protect information infrastructures. Activities in this category include educating employees in the information infrastructure that they work with, making employees aware of the threats that are facing the information infrastructure that they operate, making employees take ownership of and responsibility for their activities when using municipal information infrastructures, encouraging acceptable and ethical behaviour, and assessing how employees are complying with the cyber-security policy.

The researcher wanted to develop a theory that explains cyber-security implementation in the metropolitan municipalities in South Africa. Chapter 5 presented how a substantive theory was developed. This substantive theory integrated ideas and hypotheses that account for cyber-security implementation in the metropolitan municipalities in South Africa.

e. How can metropolitan municipalities in South Africa successfully assess their cyber-security status?

An instrument or tool is required to conduct an assessment of cyber-security status. The assessment tool must produce assessment results that guide management in the decision-making process. Chapter 6 dealt with how the researcher developed a municipal cyber-security conceptual framework from the ConGTM. Chapter 7 dealt with how, from the conceptual framework, the researcher developed an instrument to assess cyber-security.

Chapter 8 explained the detailed process of how to assess the cyber-security status in a metropolitan municipality.

The process to successfully assess the status of cyber-security in the municipality entailed the following:

- Proper communication with key stakeholders, including executive management, of business units that operate or are the custodians of critical information infrastructures. In cases where there is a cyber-security structure of function, the gateway to assess cyber-security status would be this structure as it facilitates and coordinates cyber-security activities. This is the structure that drives the agenda of the cyber-security programme within the municipality.
- Identification of participants that will participate in the assessment exercise. The participants needed to represent all relevant units that operate the information infrastructure, and moreover those that operate the critical information infrastructure. The participants needed to represent all occupational levels within those applicable participating business units.
- Deployment of cyber-security assessment tool. The tool was statistically validated, and produced credible results. Metropolitan municipalities have adopted electronic mail systems, hence the deployment of the assessment tool became easier. Also, the intranet application could be used for disseminating the cyber-security assessment instrument.
- Monitoring of the responses during the duration of the assessment. This monitoring assisted in having a holistic picture of the responses being received in terms of the numbers of participants and the participating business units. If the responses were not representative of the target population, reminders and motivating actions were considered.
- Analysing the data that was collected through the cyber-security assessment survey questionnaire instrument.
- Writing the assessment report after statistically analysing the data. The report had to be presented to pertinent management. The report had to present the as is status of cyber-security. If there were areas that required management attention, the possible risk impact associated with those control deficiencies had to be highlighted in the report, including the recommended practices to address the identified weaknesses.

The researcher developed the cyber-security assessment instrument, and statistically validated the tool in order to rely on the results that the tool generates. The research objective for this sub-question was achieved.

The study's core objective was particularly to determine the cyber-security status in South African metropolitan municipalities. Chapter 8 covered how the cyber-security assessment tool was deployed in three metropolitan municipalities in the country. Had it not been for time constraints, the cyber-security assessment instrument would have been deployed to all eight metropolitan municipalities. The assessment results were presented in Chapter 8. Each municipality that participated in the study was assessed separately and the assessment report, which contained control deficiencies, the possible risk impact for those deficiencies, and recommended corrective actions was presented to relevant management within the municipality. A consolidated report with all the three participating municipalities was also generated and was presented in Chapter 8.

9.3. RESEARCH CONTRIBUTION

The contribution of this study is twofold. The first contribution is to the body of knowledge in local government cyber-security. As highlighted in the NCPF, the national government acknowledges that in this information age cyber-security is one of the challenging areas for government at all levels. The NCPF also recognises the severe damage that cyber-security threats can cause to some government critical infrastructures, which in turn can lead to widespread disruption to government services, and or even the loss of human lives. An uncoordinated approach and siloed view of cyber-security is another important aspect that the NCPF is highlighting. As discussed in Chapter 2 of this research, the current research focus in cyber-security has not been directed on local government where there are a sizeable number of critical infrastructures that could be severely affected by weakness in cyber-security. Therefore, this research has made the following contribution:

(a) A substantive theory has been developed, which aids the understanding of what activities are conducted to advance the protection of municipal information infrastructure against cyber-security threats. The integrated development cyber-security theory is anticipated to go a long way in assisting the local sphere of government in addressing the challenge of cyber-security.

(b) A conceptual framework has been established which guides the processes to be implemented to secure the information infrastructure in a metropolitan municipality environment. Currently there is no known framework that municipal authorities can adopt to successfully implement cyber-security in the municipality. Metropolitan municipalities are the areas where there is high population density, and high economic activities. Therefore, the impact of cyber-security deficiencies could affect quite a high number of the population and the industrial activities. If appropriately applied, the developed conceptual framework could assist to minimise exposure of critical information infrastructure to cyber-security threats

(c) A statistically tested, cyber-security status assessment tool has been formulated to assist the metropolitan municipalities to evaluate their posture on cyber-security. This assessment instrument can assist the municipalities to determine the as is status of cyber-security with the intention of identifying cyber-security-related control areas that require urgent management attention in pursuit of safeguarding information infrastructure.

The second contribution of this study is made to the practitioners in the local government sphere.

- Through the emerged cyber-security conceptual framework, this study provides practical processes to be executed when implementing a cyber-security programme in the metropolitan municipality environment.
- The researcher has compiled an inventory of cyber-security controls that practitioners can adopt to protect information infrastructure against cyber threats. The key cyber-security controls that this study has suggested to be considered by practitioners include: creating an inventory of critical information infrastructure to be protected against cyber-related risks, formulating a cyber-security structure or function that will drive the agenda of cyber-security across the municipality, creating a cyber-security policy that is aligned to the municipal IDP, and continuous assessment of the cyber-security status with the aim of keeping all the role players on their toes in security information infrastructures.
- Practitioners in the metropolitan municipalities can adopt the cyber-security status assessment tool to evaluate the adequacy and effectiveness of the implemented controls to protect information infrastructure against cyber risks. The assessment

results could assist the practitioners to motivate for resource allocation (money and human resources) in addressing the identified weakness. Executive management in the metropolitan municipalities can base their decisions on the assessment report that has been created through the adoption of the credible cyber-security status assessment instrument that this research has developed. It is anticipated that the continuous assessment of the status of cyber-security will advance the culture of cyber-security in the metropolitan municipalities.

9.4. RESEARCH LIMITATIONS

- The cyber-security assessment tool that this study has developed does not cater for different occupational levels in the municipality. A question in the survey could be relevant to the head of the unit and senior management team but not important to operational staff on the ground.
- The cyber-security assessment tool does not cater for qualitative methods of data collection. Only the quantitative data collection method is used in the assessment tool. The assessment instrument does not for example cater for focused groups and interviews.

9.5. FUTURE RESEARCH

- The cyber-security assessment tool can be improved by means of qualitative data collection methods.
- The assessment tool can be tested further in other metropolitan municipalities with the intention of confirming or disputing its validity.
- The municipal cyber-security conceptual framework can be revisited to align with the current trends in information infrastructure, changes in the country's regulations and legislation, or any other new developments that could impact the framework.
- The framework and the assessment tool can be tested on other types of municipalities in the country.
- The statements in the cyber-security status assessment instrument can be improved or adapted to align with the level of the audience in the municipality being assessed

REFERENCES

Allan, G. (2007). The use of the grounded theory methodology in investigating practitioners' integration of COTS components in information systems. *ICIS 2007 Proceedings*, p. 149.

Auditor General of South Africa (AGSA). (2014). *Consolidated general report on the audit outcomes of local government 2013-14.* Pretoria: Government Printers.

Ball, K. M. (2017). African Union Convention on Cyber Security and Personal Data Protection. *International Legal Materials, 56*(1), 164-192.

Bryman, A., & Bell, E. (2007). *Business research methods*. 2nd ed. New York: Oxford University Press.

Charmaz, K. (2008). Constructionism and the grounded theory method. In J. A. Holstein, & J. F. Gubrium (eds.), *Handbook of constructionist research* (pp. 397-412). New York: The Guilford Press.

Charmaz, K. (2006). *Constructing grounded theory. A practical guide through qualitative analysis*. London: SAGE Publications.

Chen, T. (2010). Stuxnet, the real start of cyber warfare? [Editor's Note]. *IEEE Network*, vol. 24, no. 6, pp. 2-3.

Cherryholmes, C. H. (1992). Notes on pragmatism and scientific realism. *Educational researcher*, vol. 21, no. 6, pp. 13-17.

City of Tshwane. 2017. *Integrated Development Plan (IDP)*. Tshwane: Tshwane Municipality.

Clark, L. A., & Watson, D. (1995). Constructing validity: Basic issues in objective scale development. *Psychological Assessment*, vol. 7, no. 3, pp. 309-319.

Clemente, D. (2013). *Cyber security and global interdependence: What is critical?* London: Chatham House: The Royal Institute of International Affairs.

Cooper, D. R., & Schindler, P. S. (2001). *Business research methods*. Boston, MA: McGraw-Hill.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, vol. 4, no. 10, pp. 13-21.

Creswell, J. W. (2013). *Research design: Qualitative, quantitative, and mixed methods approaches.* London: Sage.

Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed method approaches*. London: Sage.

Crotty, M. (1998). *The foundations of social research: Meaning and perspective in the research process*. London: Sage Publications Limited.

De Lange, M., & Von Solms, R. (2012). *An e-Safety educational framework in South Africa*. Proceedings of the Southern Africa Telecommunication Networks and Applications Conference (SATNAC), Pretoria.

Dennis, A., Jones, R., Kildare, D., & Barclay, C. (2014). Design science approach to developing and evaluating a national cybersecurity framework for Jamaica. *The Electronic Journal of Information Systems in Developing Countries*, vol. 62, no. 1, pp. 1-18.

Dlamini, Z., & Modise, M. (2013). Cyber security awareness initiatives in South Africa: A synergy approach Case Study. *Inf. Warf. Secur. Res. Teach. Stud*, 1.

EThekwini Municipality Integrated Development Plan (ETh-IDP). (2017). Durban: EThekwini Municipality.

European Network and Information Security Agency (ENISA). (2015). *National Cyber Security Strategies: Practical Guide on Development and Execution*. EU: ENISA.

Falco, G., Viswanathan, A., Caldera, C., & Shrobe, H. (2018). A Master Attack Methodology for an AI-Based Automated Attack Planner for Smart Cities. *IEEE Access*, *6*, 48360-48373

Falliere, N., Murchu, L. O., & Chien, E. (2011). W32 Stuxnet dossier. White paper, Symantec Corporation. *Security Response*, vol. 5, no. 6, p. 29.

Fernandez, W. D., Lehmann, H., & Underwood, A. (2002). *Rigor and relevance in studies of IS Innovation: A grounded theory methodology approach*. ECIS 2002 Proceedings, Paper 134.

Glaser, B. G. (2004). Remodelling grounded theory. *The Grounded Theory Review: An International Journal*, vol. 4, no. 1, pp. 1-24.

Glaser, B. G. (1992). *Emerging vs forcing: Basics of grounded theory analysis*. Mill Valley, CA: The Sociology Press.

Glaser, B. G. (1978). *Theoretical sensitivity: Advances in the methodology of grounded theory*. Mills Valley, CA: The Sociology Press.

Glaser, B., & Strauss, A. (1967). *The discovery of grounded theory: Strategies for qualitative research.* Chicago: Aldine Publishing Company.

Global Forum on Cyber Expertise (GFCE). (2016). *The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for Governmental Policy Makers.* [Online]. Available WWW: https://www.meridianprocess.org/siteassets/meridian/gfce-meridian-gpg-to-ciip.pdf.

Grobler, M., Van Vuuren, J. J., & Leenen, L. (2012). *Implementation of a cyber-security policy in South Africa: Reflection on progress and the way forward*. IFIP International Conference on Human Choice and Computers (pp. 215-225). Berlin, Heidelberg: Springer.

Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. In N. K. Denzin, & Y. S. Lincoln (eds.), *Handbook of qualitative research* (pp. 105-117). Thousand Oaks: Sage Publications.

Hathaway, M. (2015). *Cyber readiness index 2.0. A plan for cyber readiness: A baseline and an index*. US: Potomac Institute for Policy Studies.

in.KNOW.vation. (2015). *Smart cities*. Pretoria: SALGA.

Institute of Risk Management South Africa (IRMSA). (2015). *South Africa Risk Report*. Sandton: IRMSA.

International Organization for Standardization/ Electoral Commission of South Africa (ISO/IEC). (2012). *Information technology – Security techniques – Guidelines for cybersecurity*. Geneva Switzerland: ISO/IEC.

International Telecommunication Union (ITU). (2015). *Global Cybersecurity Index & Cyberwellness Profiles*. Geneva, Switzerland: ITU.

International Telecommunication Union (ITU). (2008). *Telecommunication standardization sector of ITU: Overview of cybersecurity*. Geneva, Switzerland: ITU.

Kaplan, B., & Maxwell, J. A. (2005). Qualitative research methods for evaluating computer information systems. In J. G. Anderson, C. E. Aydin, & S. J. Jay (eds.), *Evaluating the organizational impact of healthcare information systems*. New York: Springer.

Karnouskos, S. (2011). Stuxnet worm impact on industrial cyber-physical system security. *37th Annual Conference on IEEE Industrial Electronics Society* (pp. 4490–4494). Germany: IEEE.

Kitchin, R. (2016). *Getting smarter about smart cities: Improving data privacy and data security*. Dublin, Ireland: Data Protection Unit, Department of the Taoiseach.

Klein, H. K., & Myers, M. D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly*, vol. 23, no. 1, pp. 67-94.

Kortjan, N., & Von Solms, R. (2014). A conceptual framework for cyber-security awareness and education in SA. *South African Computer Journal*, vol. 52, no. 1, pp. 29-41.

Lehmann, H. (2010). Grounded theory and information systems: Are we missing the point? *43rd Hawaii International Conference*, pp. 1-11.

Luiijf, E., Besseling, K., & De Graaf, P. (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures*, vol. 9, numbers 1-2, pp. 3-31.

Mahlobo, D. (2016, April 24). *South African State Security Agency 2016/17 Departmental Budget Vote Speech*. Pretoria: Government Printer.

Mahlobo, D. (2015, December 4). *National Cyber-security Policy Framework*. Pretoria: Government Gazette.

Matrosov, A., Rodionov, E., Harley, D., & Malcho, J. (2010). *Stuxnet under the microscope*. Spain: ESET LLC.

Miles, M., & Huberman, A. M. (1994). Qualitative data analysis: An expanded sourcebook. 2nd Edition. Thousand Oaks, CA: Sage.

Mohideen, F. (2016). The cyber-security state of our nation: A critique of South Africa's stance on cyber-security in respect of the protection of critical information infrastructure. *11th International Conference on Cyber Warfare and Security (ICCWS),* p. 235.

Morgan, D. L. (2007). Paradigm lost and pragmatism regained methodological implications of combining qualitative and quantitative methods. Journal of Mixed Method Research, vol. 1, no. 1, pp. 48-76.

National Institute of Standards and Technology (NIST). (2014). *Framework for improving critical infrastructure cybersecurity, Version 1.0*. [Online]. Available WWW: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

National Planning Commission (NPC). (2012). *National Development Plan 2030 – Our Future make it work*. South Africa: NPC.

Neitzel, L., & Huba, B. (2014). Top ten differences between ICS and IT cybersecurity. *InTech*, vol. 61, no. 3, pp. 12-18.

Nelson Mandela Bay Municipality (NMBM). 2017. *Integrated Development Plan (IDP) 2017/18–2021/22*. [Online]. Available WWW: http://www.nelsonmandelabay.gov.za/datarepository/documents/nmbm-2017-18-to-2021-22-idp.pdf.

Nelson Mandela Bay Municipality (NMBM). 2016. *Integrated Development Plan (IDP) 2016-17–2020/21*. [Online]. Available WWW: http://www.nelsonmandelabay.gov.za/datarepository/documents/adopted-2016-2021-golden-five-years-idp-june-2016-web.pdf.

Onwuegbuzie, A. J., & Collins, K. M. (2007). A typology of mixed methods sampling designs in social science research. *The Qualitative Report*, vol. 12, no. 2, pp. 281-316.

Organisation for Economic Co-operation and Development (OECD). (2015). *Digital security risk management for economic and social prosperity: OECD recommendation and companion document*. Paris: OECD Publishing.

Orji, U. J. (2018). The African Union Convention on Cybersecurity: A Regional response towards Cyber Stability? *Masaryk University Journal of Law and Technology*, *12*(2), 91-130.

Oxford Dictionary. (2006). *Oxford advanced learner's dictionary*. International student's edition. Oxford: Oxford University Press.

Patton, M. (1990). *Qualitative evaluation and research methods*. Newbury Park, CA: Sage.

Phahlamohlaka, L. J., Jansen van Vuuren, J. C., & Coetzee, A. J. (2011). *Cyber security awareness toolkit for national security: An approach to South Africa's cyber security policy implementation*. Pretoria: CSIR.

Ralston, P. A., Graham, J. H., & Hieb, J. L. (2007). Cyber security risk assessment for SCADA and DCS networks. *ISA transactions*, vol. 46, no. 4, pp. 583-594.

Republic of South Africa (RSA). (2016). *Cybercrimes and Cybersecurity Bill*. Pretoria: Government Printer.

Republic of South Africa (RSA). (2006). *Independent Communications Authority of South Africa (ICASA) Amendment Act No. 3 of 2006*. Pretoria: Government Printer.

Republic of South Africa (RSA). (2003). *Municipal Finance Management Act, Act no. 56 of 2003*. Pretoria: Government Printer.

Republic of South Africa (RSA). (2002). *Electronic Communications and Transactions Act, Act No. 25 of 2002*. [Online]. Available WWW: http://www.up.ac.za/media/shared/409/ZP_Files/25-of-2002-electronic-communications-and-transactions-act_31-ma.zp44223.pdf.

Republic of South Africa (RSA). (2000). *Municipal Systems Act, Act 32 of 2000*. Pretoria: Government Gazette.

Republic of South Africa (RSA). (1998). *Local Government: Municipal Structures Act*. Pretoria: Government Printer.

Republic of South Africa (RSA). (1996).*Constitution of the Republic of South Africa, Act no. 108 of 1996*. Pretoria: Government Printer.

Sarantakos, S. (2005). *Social research*. Hampshire: Palgrave Macmillan.

Scott, K. W. (2004). Relating the categories in Grounded Theory Analysis: Using a conditional relationship guide and reflective coding matrix. *The Qualitative Report*, vol. 9, no. 1, pp. 112-126.

Strauss, A. (1987). *Qualitative analysis for social scientists*. New York: Cambridge University Press.

Strauss, A., & Corbin, J. (1998). *Basics of qualitative research: Procedures and techniques for developing grounded theory*. Thousand Oaks, CA: Sage Publications.

Strauss, A., & Corbin, J. (1990). *Basics of qualitative research, grounded theory, procedures and techniques.* London: Sage.

Symantec. (2016a). *Internet Security Threat Report*. [Online]. Available WWW: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf.

Symantec. (2016b). *Cyber crime & cyber security*. [Online] Available WWW: https://www.thehaguesecuritydelta.com/media/com_hsd/report/135/document/Cyber-security-trends-report-Africa-en.pdf.

Terre Blanche, M., Durrheim, K., & Painter, D. (2006). *Research in practice: applied methods for the social sciences*. Cape Town: University of Cape Town Press.

Urquhart, C. (2007). *The evolving nature of grounded theory method: The case of the information systems discipline*. London: Sage.

Urquhart, C., & Fernandez, W. (2013). Using grounded theory method in information systems: The researcher as blank slate and other myths. *Journal of Information Technology*, vol. 28, no. 3, pp. 224-236.

Urquhart, C., Lehmann, H., & Myers, M. D. (2010). Putting the 'theory' back into grounded theory: Guidelines for grounded theory studies in information systems. *Information Systems Journal*, vol. 20, no. 4, pp. 357-381.

Van Vuuren, J. J., Leenen, L., & Zaaiman, J. (2014). *Using an ontology as a model for the implementation of the national cybersecurity policy framework for South Africa*. ICCWS2014 – 9th International Conference on Cyber Warfare & Security (p. 107). Pretoria: Academic Conferences Limited.

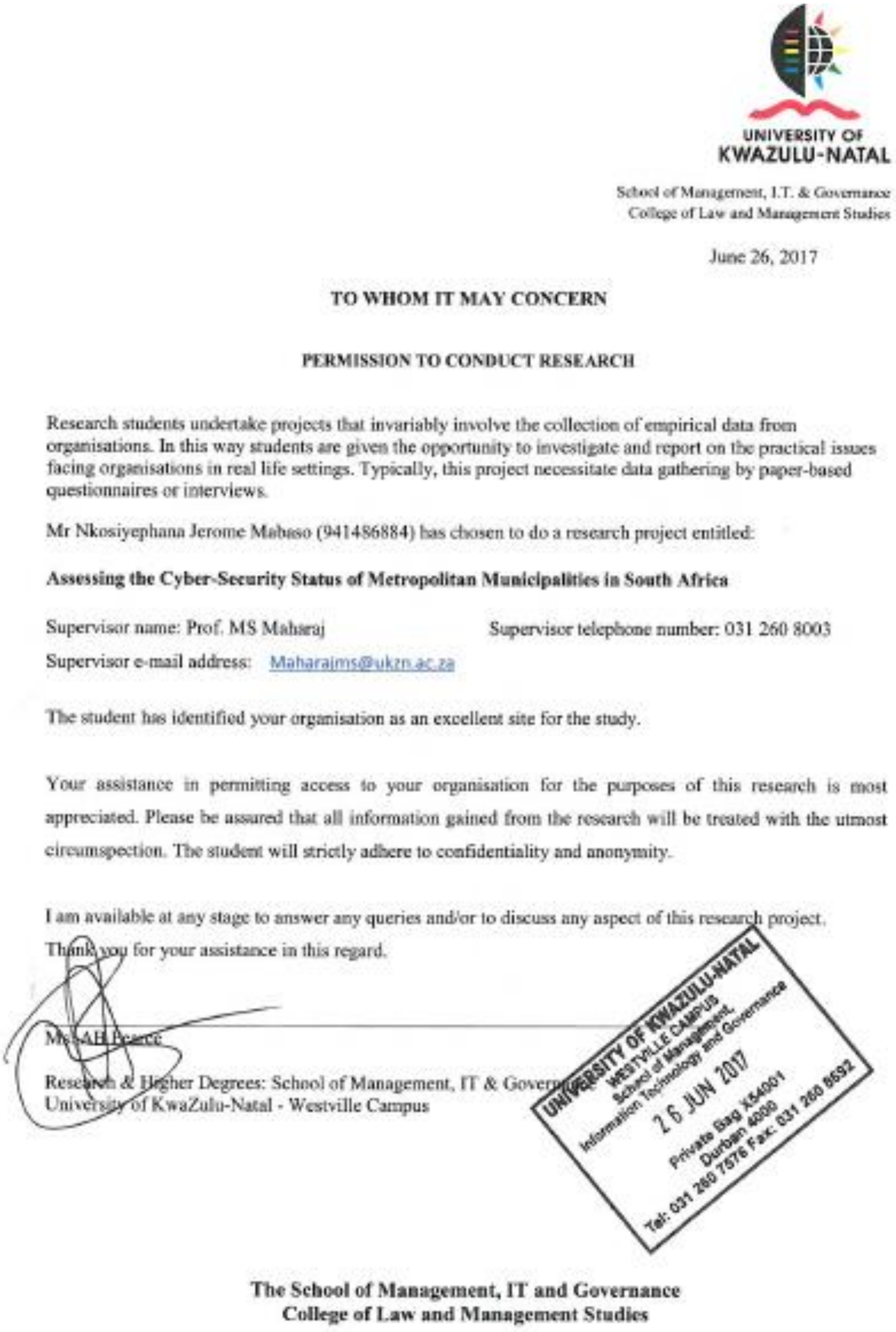
Von Solms, R., & Von Solms, B. (2015). *National Cyber Security in South Africa: A letter to the minister of cyber security*. Proceedings of the 10th International Conference on Cyber Warfare and Security, Kruger National Park, South Africa, April.

Walsham, G. (1995). Interpretive case studies in IS research: Nature and method. *European Journal of Information Systems*, vol. 4, no. 2, pp. 4-81.

Wamala, F. (2011). *ITU National Cyber Security Strategy Guide*. [Online]. Available WWW: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf.

APPENDIX A:

PERMISSION TO CONDUCT RESEARCH



UNIVERSITY OF
KWAZULU-NATAL

School of Management, I.T. & Governance
College of Law and Management Studies

June 26, 2017

TO WHOM IT MAY CONCERN

PERMISSION TO CONDUCT RESEARCH

Research students undertake projects that invariably involve the collection of empirical data from organisations. In this way students are given the opportunity to investigate and report on the practical issues facing organisations in real life settings. Typically, this project necessitate data gathering by paper-based questionnaires or interviews.

Mr Nkosiyephana Jerome Mabaso (941486884) has chosen to do a research project entitled:

Assessing the Cyber-Security Status of Metropolitan Municipalities in South Africa

Supervisor name: Prof. MS Maharaj   Supervisor telephone number: 031 260 8003

Supervisor e-mail address: Maharajms@ukzn.ac.za

The student has identified your organisation as an excellent site for the study.

Your assistance in permitting access to your organisation for the purposes of this research is most appreciated. Please be assured that all information gained from the research will be treated with the utmost circumspection. The student will strictly adhere to confidentiality and anonymity.

I am available at any stage to answer any queries and/or to discuss any aspect of this research project.

Thank you for your assistance in this regard.

Ms AH Pearce

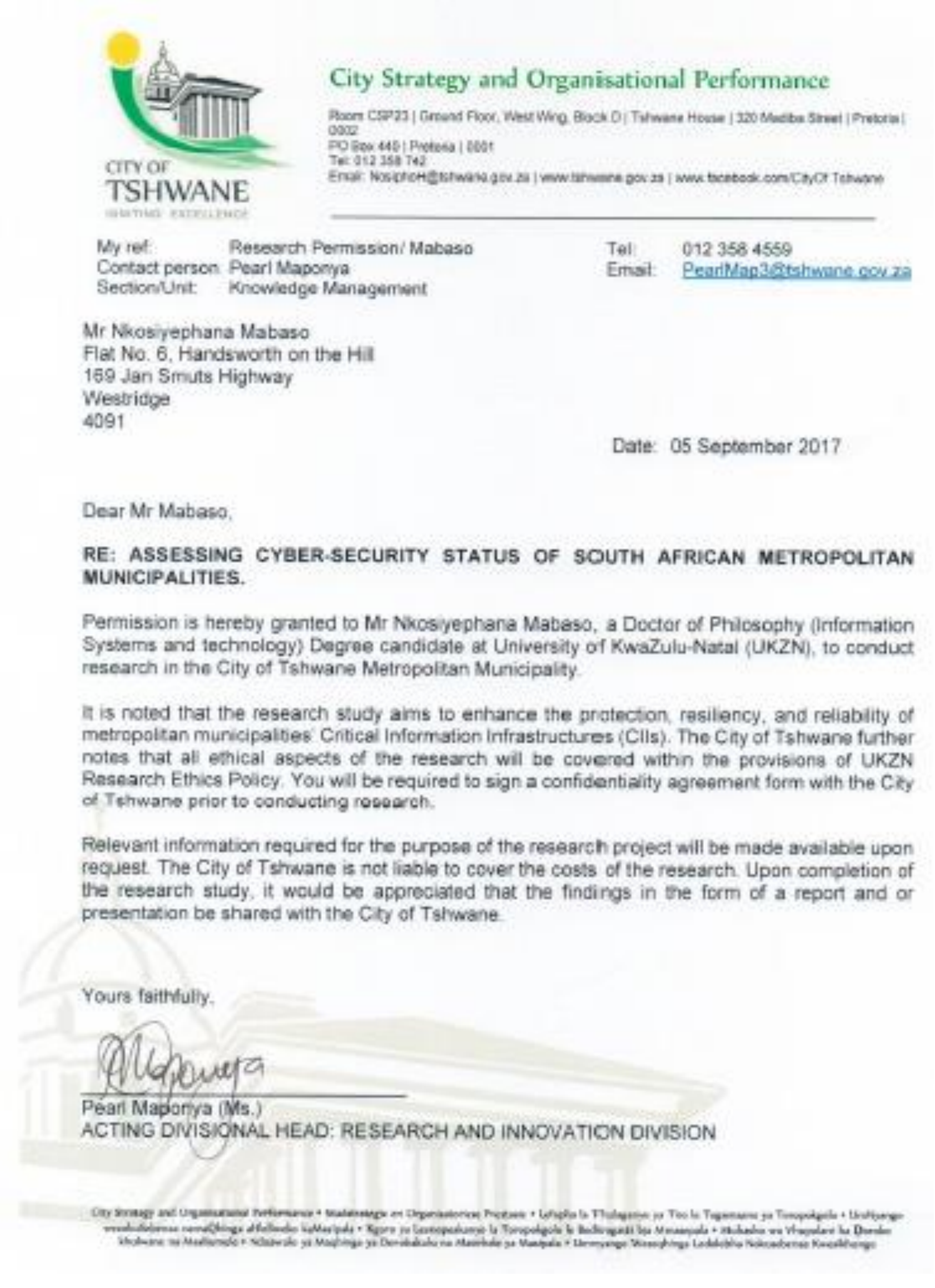
Research & Higher Degrees: School of Management, IT & Governance
University of KwaZulu-Natal - Westville Campus

UNIVERSITY OF KWAZULU-NATAL
WESTVILLE CAMPUS
School of Management,
Information Technology and Governance
2 6 JUN 2017
Private Bag X54001
Durban 4000
Tel: 031 260 7576 Fax: 031 260 8692

The School of Management, IT and Governance
College of Law and Management Studies

APPENDIX B:

APPROVED PERMISSION LETTER



CITY OF
TSHWANE

City Strategy and Organisational Performance

Room CSP23 | Ground Floor, West Wing, Block D | Tshwane House | 320 Madiba Street | Pretoria | 0002
PO Box 440 | Pretoria | 0001
Tel: 012 358 742
Email: NosiphoH@tshwane.gov.za | www.tshwane.gov.za | www.facebook.com/CityOf Tshwane

My ref:	Research Permission/ Mabaso	Tel:	012 358 4559
Contact person:	Pearl Maponya	Email:	PearlMap3@tshwane.gov.za
Section/Unit:	Knowledge Management		

Mr Nkosiyephana Mabaso
Flat No. 6, Handsworth on the Hill
169 Jan Smuts Highway
Westridge
4091

Date: 05 September 2017

Dear Mr Mabaso,

RE: ASSESSING CYBER-SECURITY STATUS OF SOUTH AFRICAN METROPOLITAN MUNICIPALITIES.

Permission is hereby granted to Mr Nkosiyephana Mabaso, a Doctor of Philosophy (Information Systems and technology) Degree candidate at University of KwaZulu-Natal (UKZN), to conduct research in the City of Tshwane Metropolitan Municipality.

It is noted that the research study aims to enhance the protection, resiliency, and reliability of metropolitan municipalities' Critical Information Infrastructures (CIIs). The City of Tshwane further notes that all ethical aspects of the research will be covered within the provisions of UKZN Research Ethics Policy. You will be required to sign a confidentiality agreement form with the City of Tshwane prior to conducting research.

Relevant information required for the purpose of the research project will be made available upon request. The City of Tshwane is not liable to cover the costs of the research. Upon completion of the research study, it would be appreciated that the findings in the form of a report and or presentation be shared with the City of Tshwane.

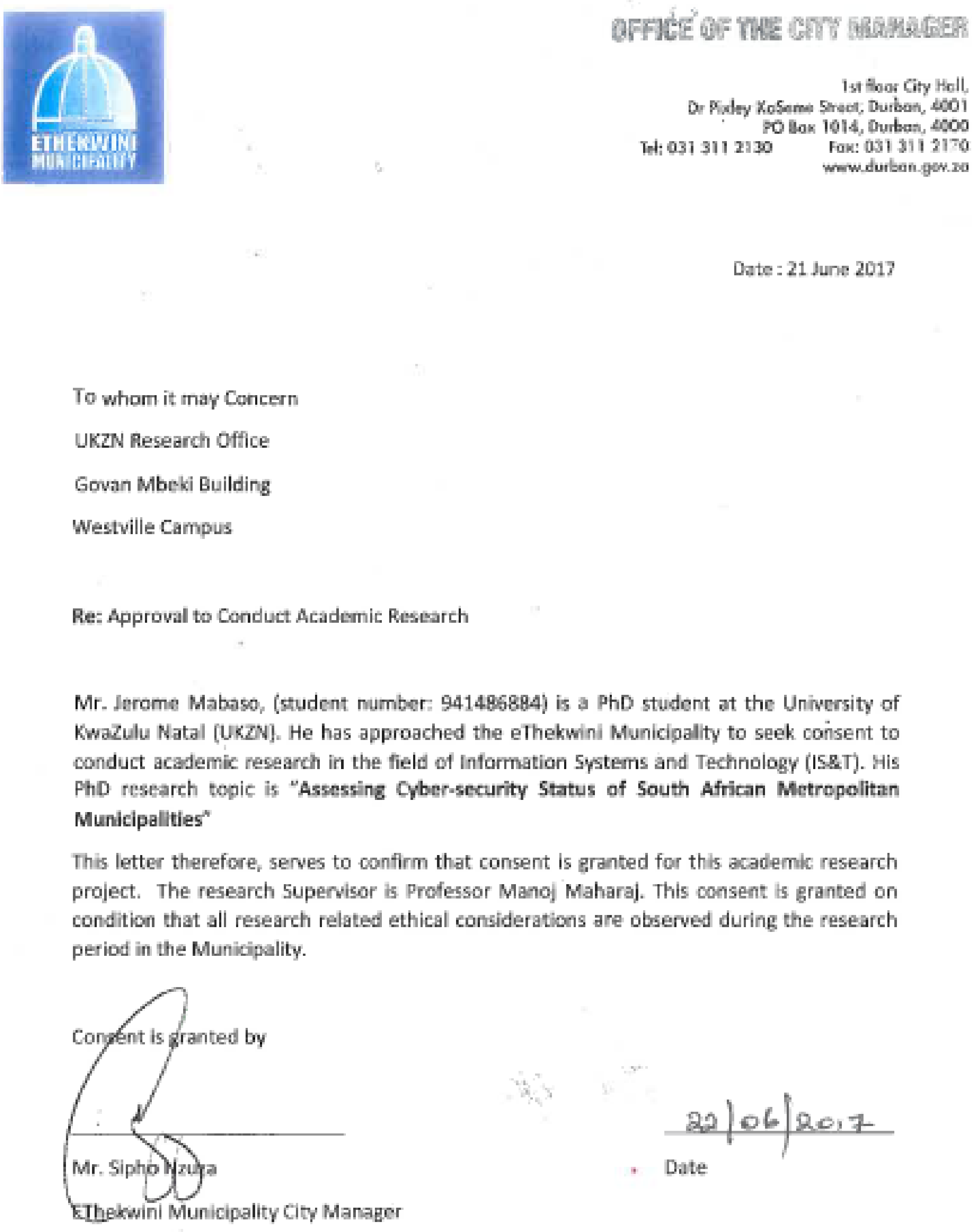
Yours faithfully,

Pearl Maponya (Ms.)
ACTING DIVISIONAL HEAD: RESEARCH AND INNOVATION DIVISION

City Strategy and Organisational Performance • Stadstrategie en Organisatoriese Prestasie • [illegible]

APPENDIX C:

GATEKEEPER'S LETTER: ETHEKWINI MUNICIPALITY



ETHEKWINI MUNICIPALITY

OFFICE OF THE CITY MANAGER

1st floor City Hall,
Dr Pixley KaSeme Street, Durban, 4001
PO Box 1014, Durban, 4000
Tel: 031 311 2130 Fax: 031 311 2170
www.durban.gov.za

Date : 21 June 2017

To whom it may Concern

UKZN Research Office

Govan Mbeki Building

Westville Campus

Re: Approval to Conduct Academic Research

Mr. Jerome Mabaso, (student number: 941486884) is a PhD student at the University of KwaZulu Natal (UKZN). He has approached the eThekwini Municipality to seek consent to conduct academic research in the field of Information Systems and Technology (IS&T). His PhD research topic is "**Assessing Cyber-security Status of South African Metropolitan Municipalities**"

This letter therefore, serves to confirm that consent is granted for this academic research project. The research Supervisor is Professor Manoj Maharaj. This consent is granted on condition that all research related ethical considerations are observed during the research period in the Municipality.

Consent is granted by

Mr. Sipho Nzuza

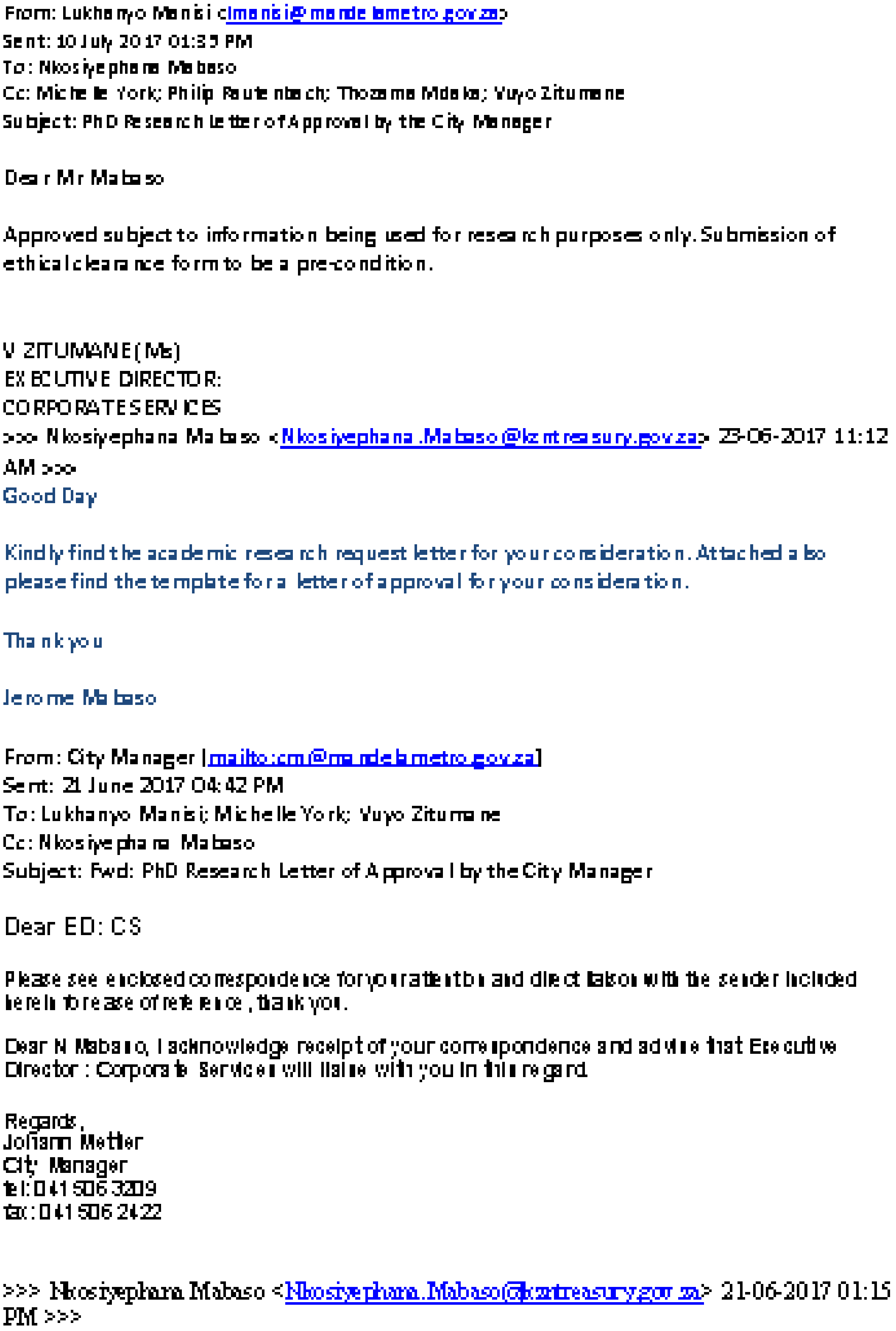
EThekwini Municipality City Manager

22/06/2017

Date

APPENDIX D:

GATEKEEPER'S LETTER: NELSON MANDELA BAY



From: Lukhanyo Manisi <lmanisi@mandelametro.gov.za>
Sent: 10 July 2017 01:35 PM
To: Nkosiyephana Mabaso
Cc: Michelle York; Philip Rautenbach; Thozama Mdaka; Vuyo Zitumane
Subject: PhD Research letter of Approval by the City Manager

Dear Mr Mabaso

Approved subject to information being used for research purposes only. Submission of ethical clearance form to be a pre-condition.

V ZITUMANE (Ms)
EXECUTIVE DIRECTOR:
CORPORATE SERVICES
>>> Nkosiyephana Mabaso <Nkosiyephana.Mabaso@kzntreasury.gov.za> 23-06-2017 11:12 AM >>>
Good Day

Kindly find the academic research request letter for your consideration. Attached also please find the template for a letter of approval for your consideration.

Thank you

Jerome Mabaso

From: City Manager [mailto:cm@mandelametro.gov.za]
Sent: 21 June 2017 04:42 PM
To: Lukhanyo Manisi; Michelle York; Vuyo Zitumane
Cc: Nkosiyephana Mabaso
Subject: Fwd: PhD Research Letter of Approval by the City Manager

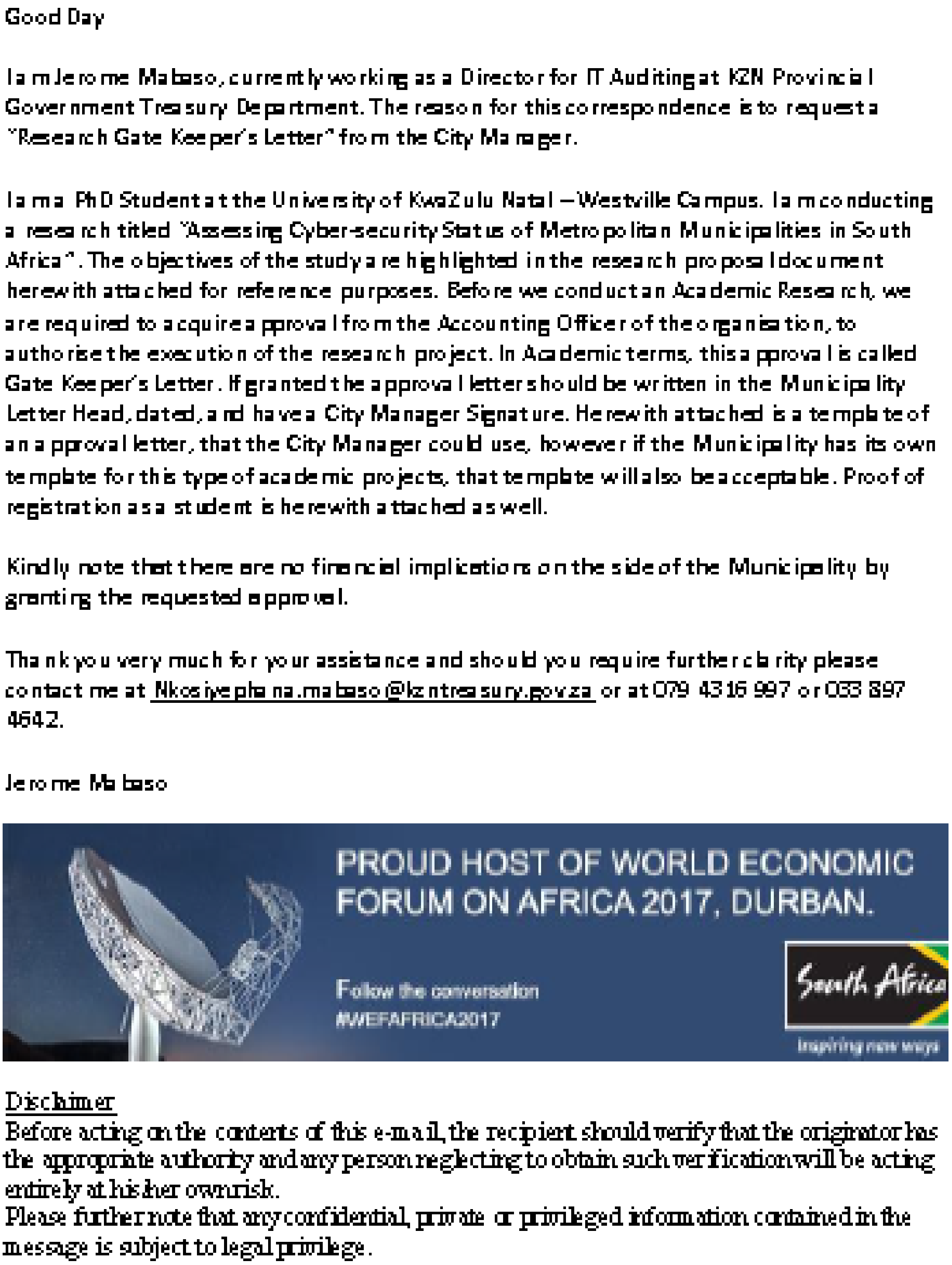
Dear ED: CS

Please see enclosed correspondence for your attention and direct liaison with the sender included herein for ease of reference, thank you.

Dear N Mabaso, I acknowledge receipt of your correspondence and advise that Executive Director : Corporate Services will liaise with you in this regard.

Regards,
Johann Mettler
City Manager
tel: 041 506 3209
fax: 041 506 2422

>>> Nkosiyephana Mabaso <Nkosiyephana.Mabaso@kzntreasury.gov.za> 21-06-2017 01:15 PM >>>



Good Day

I am Jerome Mabaso, currently working as a Director for IT Auditing at KZN Provincial Government Treasury Department. The reason for this correspondence is to request a "Research Gate Keeper's Letter" from the City Manager.

I am a PhD Student at the University of KwaZulu Natal – Westville Campus. I am conducting a research titled "Assessing Cyber-security Status of Metropolitan Municipalities in South Africa". The objectives of the study are highlighted in the research proposal document herewith attached for reference purposes. Before we conduct an Academic Research, we are required to acquire approval from the Accounting Officer of the organisation, to authorise the execution of the research project. In Academic terms, this approval is called Gate Keeper's Letter. If granted the approval letter should be written in the Municipality Letter Head, dated, and have a City Manager Signature. Herewith attached is a template of an approval letter, that the City Manager could use, however if the Municipality has its own template for this type of academic projects, that template will also be acceptable. Proof of registration as a student is herewith attached as well.

Kindly note that there are no financial implications on the side of the Municipality by granting the requested approval.

Thank you very much for your assistance and should you require further clarity please contact me at Nkosiyephana.mabaso@kzntreasury.gov.za or at 079 4316 997 or 033 897 4642.

Jerome Mabaso

Disclaimer
Before acting on the contents of this e-mail, the recipient should verify that the originator has the appropriate authority and any person neglecting to obtain such verification will be acting entirely at his/her own risk.
Please further note that any confidential, private or privileged information contained in the message is subject to legal privilege.

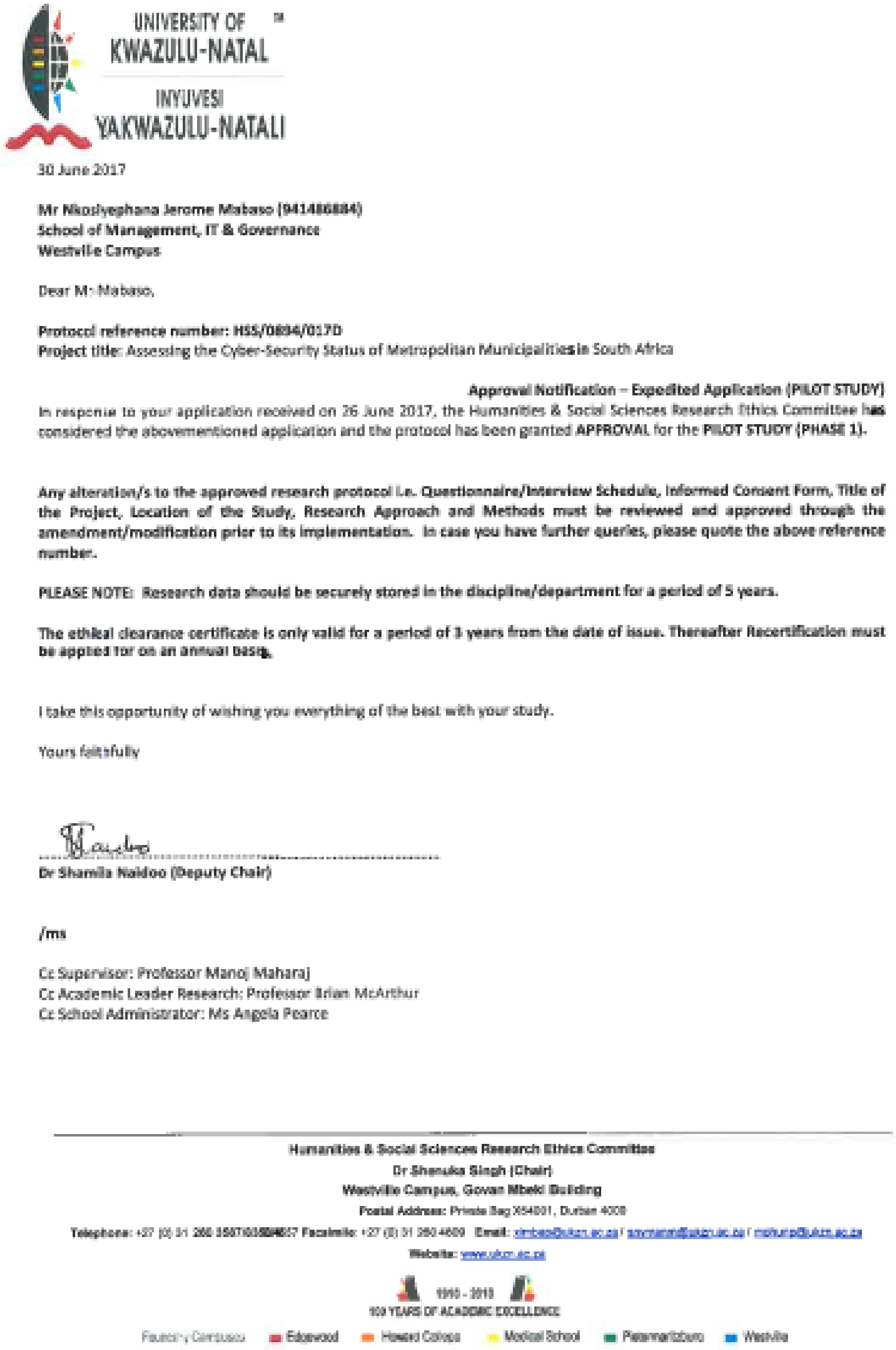
Disclaimer

Before acting on the contents of this e-mail, the recipient should verify that the originator has the appropriate authority and any person neglecting to obtain such verification will be acting entirely at his/her own risk.

Please further note that any confidential, private or privileged information contained in the message is subject to legal privilege.

APPENDIX E:

APPROVED NOTIFICATION: PILOT STUDY



UNIVERSITY OF KWAZULU-NATAL

INYUVESI YAKWAZULU-NATALI

30 June 2017

Mr Nkosiyephana Jerome Mabaso (941486884)
School of Management, IT & Governance
Westville Campus

Dear Mr Mabaso,

Protocol reference number: HSS/0894/017D
Project title: Assessing the Cyber-Security Status of Metropolitan Municipalitiesin South Africa

Approval Notification – Expedited Application (PILOT STUDY)

In response to your application received on 26 June 2017, the Humanities & Social Sciences Research Ethics Committee has considered the abovementioned application and the protocol has been granted **APPROVAL** for the **PILOT STUDY (PHASE 1).**

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

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

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

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

Yours faithfully

....

Dr Shamila Naidoo (Deputy Chair)

/ms

Cc Supervisor: Professor Manoj Maharaj
Cc Academic Leader Research: Professor Brian McArthur
Cc School Administrator: Ms Angela Pearce

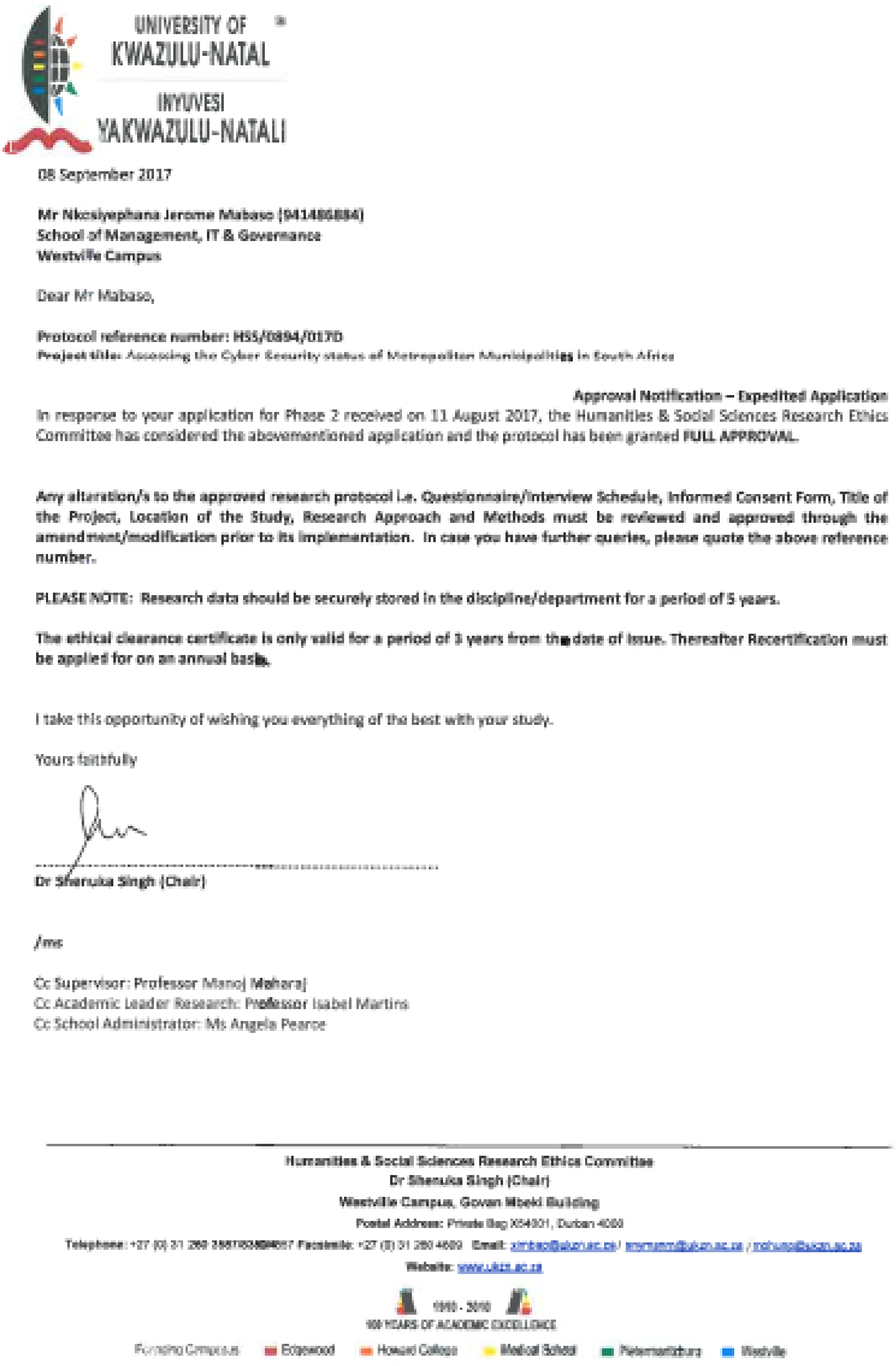
Humanities & Social Sciences Research Ethics Committee
Dr Shenuka Singh (Chair)
Westville Campus, Govan Mbeki Building
Postal Address: Private Bag X54001, Durban 4000
Telephone: +27 (0) 31 260 3587/8350/4557 **Facsimile:** +27 (0) 31 260 4609 **Email:** ximbap@ukzn.ac.za / snymanm@ukzn.ac.za / mohunp@ukzn.ac.za
Website: www.ukzn.ac.za

1910 - 2010
100 YEARS OF ACADEMIC EXCELLENCE

Founding Campuses: 🟥 Edgewood 🟧 Howard College 🟨 Medical School 🟩 Pietermaritzburg 🟦 Westville

APPENDIX F:

APPROVED NOTIFICATION: FULL APPROVAL



UNIVERSITY OF KWAZULU-NATAL

INYUVESI YAKWAZULU-NATALI

08 September 2017

Mr Nkosiyephana Jerome Mabaso (941486884)
School of Management, IT & Governance
Westville Campus

Dear Mr Mabaso,

Protocol reference number: HSS/0894/017D
Project title: Assessing the Cyber Security status of Metropolitan Municipalities in South Africa

Approval Notification – Expedited Application

In response to your application for Phase 2 received on 11 August 2017, the Humanities & Social Sciences Research Ethics Committee has considered the abovementioned application and the protocol has been granted **FULL APPROVAL.**

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

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

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

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

Yours faithfully

....
Dr Shenuka Singh (Chair)

/ms

Cc Supervisor: Professor Manoj Maharaj
Cc Academic Leader Research: Professor Isabel Martins
Cc School Administrator: Ms Angela Pearce

Humanities & Social Sciences Research Ethics Committee
Dr Shenuka Singh (Chair)
Westville Campus, Govan Mbeki Building
Postal Address: Private Bag X54001, Durban 4000
Telephone: +27 (0) 31 260 3587/8350/4557 **Facsimile:** +27 (0) 31 260 4609 **Email:** ximbap@ukzn.ac.za / snymanm@ukzn.ac.za / mohunp@ukzn.ac.za
Website: www.ukzn.ac.za

1910 - 2010
100 YEARS OF ACADEMIC EXCELLENCE

Founding Campuses: ■ Edgewood ■ Howard College ■ Medical School ■ Pietermaritzburg ■ Westville

APPENDIX G:

SURVEY QUESTIONNAIRE

Metropolitan Municipality Cyber-security Assessment Survey Questionnaire						
Legend: SA = Strongly Agree, A = Agree, DK = Don't Know, D = Disagree, SD = Strongly Disagree						
INTEGRATED DEVELOPMENT CYBER-SECURITY DOMAIN						
	Please chose the statement that best describe your view					
		YES **1**	**NO** **0**	**DON'T KNOW** **2**		
1.	My organisation has a written cyber-security policy					
2.	My organisation has an overarching supply chain management policy that guide the acquisition of information infrastructure					
3.	My organisation has a documented cyber-security strategy					
4.	My organisation has an inventory of critical information infrastructure					
5.	My organisation has information infrastructures contingency plans					
		SA **5**	**A** **4**	**DK** **3**	**D** **2**	**SD** **1**
6.	The cyber-security policy is constantly reviewed to incorporate emerging trends in the protection of information infrastructures					
7.	The cyber-security policy contains sections that are relevant to my job					
8.	The cyber-security policy is aligned to the Municipal Integrated Development Plan (IDP)					
9.	I believe our Cyber-security strategy is aligned to the Municipal IDP					
10.	There is a structure or unit within my organisation that is responsible to implement the cyber-security strategy					
11.	I know what to do if I want to report breaches or violations against cyber-security policy					
12.	I know who the custodian of the cyber-security policy is					
13.	My organisation conducts research and development with the aim to enhance protection of information infrastructure					
14.	Protection of information infrastructure in my organisation is guided by the industry best practices					

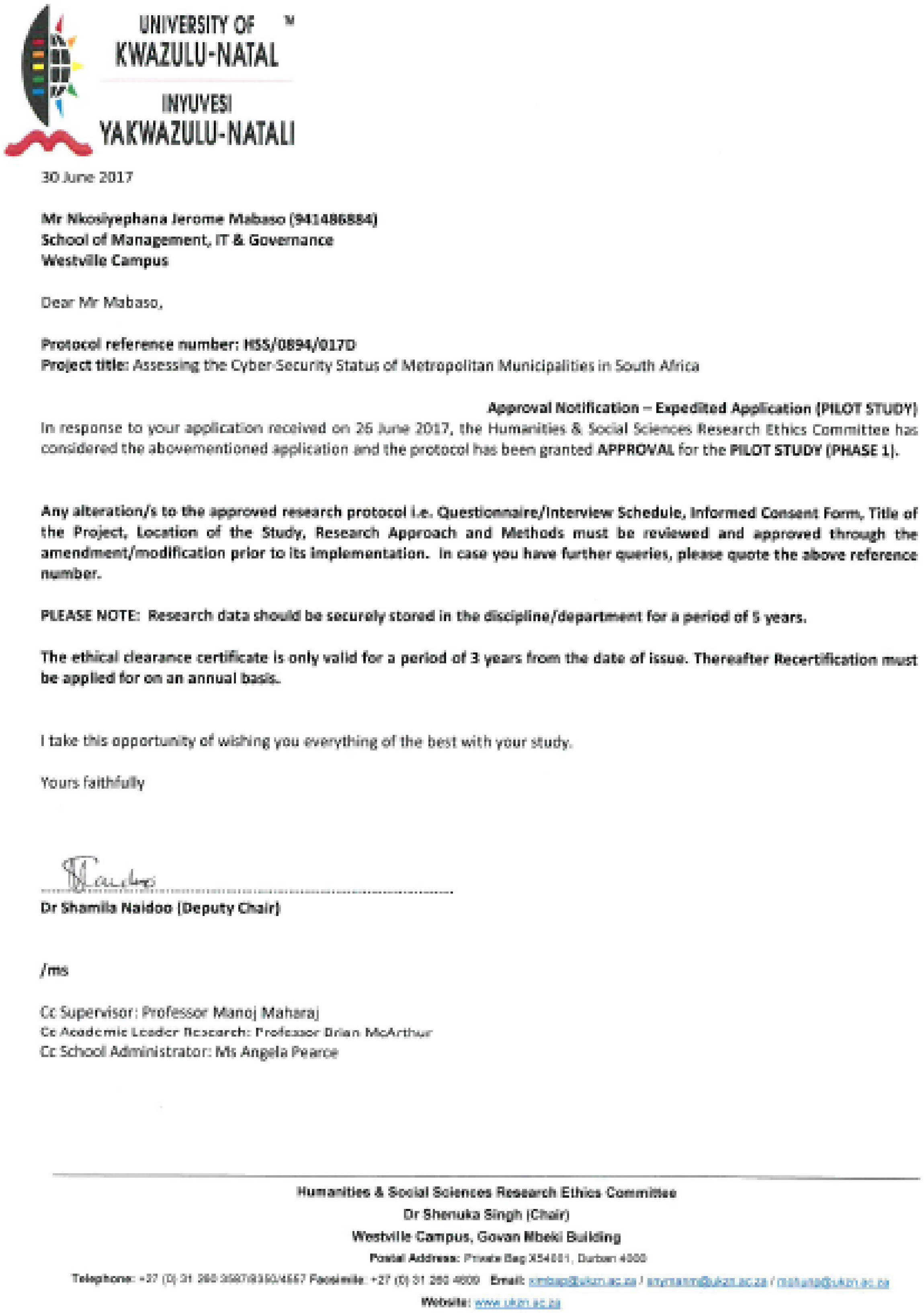
CYBER-SECURITY GOVERNANCE DOMAIN						
		YES **1**	**NO** **0**	**DON’T KNOW** **2**		
15.	My organisational strategic risk register contains cyber-security risk					
		SA **5**	**A** **4**	**DK** **3**	**D** **2**	**SD** **1**
16.	Management has allocated adequate budget to implement cyber-security policy					
17.	Risk Management processes guide the implementation of cyber-security controls in my organisation					
18.	Management has provided guidance on the regulatory requirements pertaining to information infrastructure that I work with					
19.	Management has allocated adequate people to protection information infrastructures					
20.	Management enforces compliance to cyber-security					
21.	In my organisation there are oversight structures / committees that hold management to account for the protection of information infrastructure					
22.	Internal Audit operational plans incorporate audits or reviews on information infrastructures on an annual basis					
23.	Management have input in the Internal Audit operational plans before the plan is implemented					
24.	Audit Committee approves the internal audit operational plans before the plan is implemented					
25.	Management has implemented clear asset management practices.					
26.	Management understands the possible impact of cyber-security threats to Municipal service delivery					
CYBER-SECURITY TECHNICAL OPERATIONS DOMAIN						
		YES **1**	**NO** **0**	**DON’T KNOW** **2**		
27.	There are service level agreements between my Municipality and the service providers working on information infrastructures					
		SA **5**	**A** **4**	**DK** **3**	**D** **2**	**SD** **1**
28.	Management is monitoring the services provided by the service providers / consultants against the service level agreements					

29.	My organisation has deployed technologies to protect information infrastructures against cyber threats					
30.	Access to information infrastructures is controlled through identification and authentication					
31.	Management has adopted industry best practices to protect information infrastructure against cyber-threats					
32.	Anti-virus software are installed into our laptops, desktops, and other devices					
33.	Audits are conducted to provide assurance on the adequacy and effectiveness of controls that have been implemented to protect information infrastructure					
34.	The incident management procedures are adequate to resolve cyber-security incidents					
35.	The building that I work in is adequately protected to secure the information infrastructure					
MANAGE HUMAN ISSUES IN CYBER-SECURITY DOMAIN						
		SA **5**	**A** **4**	**DK** **3**	**D** **2**	**SD** **1**
36.	Employees' activities on information infrastructure are monitored					
37.	In my organisation action is taken against employees who violate cyber-security policy					
38.	Employees are made aware of the cyber-security policy contents					
39.	Employees know where to report suspicious illicit cyber-security activities					
40.	Employees receive adequate training in the information infrastructure they operate					
41.	I am aware of cyber-security threats affecting the information assets I work with					
42.	I am aware that organisational Internet and e-mail systems should be used for business purposes					
43.	Employees accept responsibility towards information infrastructure protection					
44.	My organisation constantly conducts cyber-security assessment to determine how employees are complying with the cyber-security policy					
BIOGRAPHICAL INFORMATION						
45.	I have been in the employ of the Municipality for	• Less than 3 years = 1 • 3 years but less than 5 years = 2 • 5 years but less than 7 years = 3				

		• 7 years but less than 10 years = 4 • 10 years and over = 5
46.	I belong to	• Information and Communication Technology Category = 1 • Operating Technology = 2 • Administration Category = 3
47.	My position is at	• Management level = 1 • Specialist level = 2 • Clerical level = 3

APPENDIX H:

ETHICAL CLEARANCE LETTER



UNIVERSITY OF KWAZULU-NATAL™

INYUVESI YAKWAZULU-NATALI

30 June 2017

Mr Nkosiyephana Jerome Mabaso (941486884)
School of Management, IT & Governance
Westville Campus

Dear Mr Mabaso,

Protocol reference number: HSS/0894/017D
Project title: Assessing the Cyber-Security Status of Metropolitan Municipalities in South Africa

Approval Notification – Expedited Application (PILOT STUDY)

In response to your application received on 26 June 2017, the Humanities & Social Sciences Research Ethics Committee has considered the abovementioned application and the protocol has been granted **APPROVAL** for the **PILOT STUDY (PHASE 1).**

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

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

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

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

Yours faithfully

....

Dr Shamila Naidoo (Deputy Chair)

/ms

Cc Supervisor: Professor Manoj Maharaj
Cc Academic Leader Research: Professor Brian McArthur
Cc School Administrator: Ms Angela Pearce

Humanities & Social Sciences Research Ethics Committee
Dr Shenuka Singh (Chair)
Westville Campus, Govan Mbeki Building
Postal Address: Private Bag X54001, Durban 4000
Telephone: +27 (0) 31 260 3587/8350/4557 **Facsimile:** +27 (0) 31 260 4609 **Email:** ximbap@ukzn.ac.za / snymanm@ukzn.ac.za / mohunp@ukzn.ac.za
Website: www.ukzn.ac.za